Data Processing Addendum

The parties conclude this Data Processing Addendum ("DPA"), which forms part of the Agreement between Customer and Supplier, to reflect our agreement about the Processing of Personal Data, in accordance with the requirements of Data Protection Laws and Regulations, including the GDPR and the CCPA, to the extent applicable. To the extent Supplier, in providing the Services set forth in the Agreement, processes Personal Data on behalf of Customer, the provisions of this DPA apply.

References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

This DPA consists of two parts: (i) the main body of this DPA, and (ii) Attachments 1, 2, 3 and 4 hereto.

How to Execute this DPA:

1. To complete this DPA, you should:
   a. Sign the main body of this DPA in the signature box below.
   b. Complete any missing information and sign Attachment 1, Attachment 2, Attachment 3, and Attachment 4. Attachment 4 applies, if you are a Data Controller within the ambit of Article 3 GDPR.

2. Submit the completed and signed DPA to Supplier via email to dpa@epignosishq.com. Upon receipt of your validly completed DPA, this DPA will be legally binding (provided that you have not overwritten or modified any of the terms beyond completing the missing information).

How this DPA Applies

If the Customer signing this DPA is a party to the Agreement, then this DPA is an addendum to and forms part of the Agreement.

If the Customer entity signing this DPA has submitted Schedule A pursuant to the Agreement, then this DPA is an addendum to that Schedule A and applicable renewal terms.

If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is party to the Agreement executes this DPA.

This DPA shall not replace any comparable or additional rights relating to Processing of Personal Data contained in the Agreement. For the avoidance of doubt, it is stated that this DPA prevails for all issues it regulates.

Data Processing Terms

Customer and Epignosis hereby agree to the following provisions with respect to any Personal Data processed by Epignosis in relation to the provision of the Services under the Agreement.

1. DEFINITIONS

   “Adequacy Decision” means a European Commission Decision that a third country or an international organization ensures an adequate level of data protection within the meaning of Article 45 (9) GDPR in conjunction with Article 25 (6) of Directive 95/46/EC, or within the meaning of Article 45 (3) GDPR, as applicable.

   “Authorized Affiliate” means any of Customer’s Affiliate(s), which (i) is/are subject to Customer’s Binding Corporate Rules or to similar contractual clauses, including Standard Contractual Clauses or contractual clauses approved by a Supervisory Authority, where applicable, with the Customer to ensure adequate level of protection of Personal Data, (ii) is not established in a Restricted Third Country, and (iii) is permitted to use the Services pursuant to the Agreement between Customer and Epignosis, but is not a signatory Party to the Agreement and is not a “Customer” as defined under the Agreement.

   “Binding Corporate Rules” are binding internal rules that regulate the transfer of Personal Data within an organization which, where applicable, have been approved by a competent Supervisory Authority as providing an adequate level of protection to Personal Data.

   “CCPA” means the California Consumer Privacy Act (CAL. CIV. CODE § 1798.100 et. seq.) and its implementing regulations.

   “Dashboard” for applicable Services, means the user interface features of the hosted Software (as described in the Agreement);
“Data Controller” means the entity that determines the purposes and means of the Processing of Personal Data, as defined in the GDPR, and has the same meaning as “business,” as that term is defined by the CCPA.

“Data Processor” means the entity which Processes Personal Data on behalf of the Data Controller, as defined in the GDPR, and has the same meaning as “service provider,” as that term is defined by the CCPA.

“Data Protection Laws and Regulations” means all laws and regulations applicable to the Processing of Personal Data as part of or in connection with the Services, including but not limited to (i) laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR, ii) Adequacy Decisions and (iii) the CCPA, as either of (i) or (ii) or (iii) may be amended and are in force from time to time;

“Data Subject” means the individual to whom Personal Data relates, as defined in the GDPR, and has the same meaning as “consumer” as that term is defined under the CCPA;

“Epignosis” means the Supplier, and its Affiliates engaged in the Processing as these are mentioned under Clause 5.1 (i);

“Epignosis's Representative” means a natural or legal person established in the European Union who is designated by and represents Epignosis with regard to its respective obligations under the GDPR, as applicable. Epignosis’s Representative is the Greek Branch of Epignosis UK Ltd, established in Athens, Lykourgo 1, 10551, (+30) 211 800 6449;

“GDPR” means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation), as may be amended from time to time;

“Personal Data” means data about a natural person processed by Epignosis in relation to the provision of the Services under the Agreement, from which that person is identified or identifiable, and has the same meaning as “personal information” as that term is defined under the CCPA.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, blocking, erasure or destruction, as defined in the GDPR;

“Restricted Third Country” means a country to which a transfer of Personal Data, or from which access to Personal Data, would be prohibited by applicable Data Protection Laws and Regulations;

“Standard Contractual Clauses” means contractual clauses adopted by the European Commission based on Article 46 (5) GDPR in conjunction with Article 26 (4) of Directive 95/46/EC, or within the meaning of Article 46 (2) c) or d) GDPR, as applicable;

“Sub-processor” means any other processor, engaged by the Supplier, who agrees to receive from Supplier Personal Data exclusively intended for the Processing to be carried out on behalf of the Customer, in accordance with its instructions, the terms of the DPA, and the terms of the written Sub-processor contract;

“Supervisory Authority” means an independent public authority which is established by an EU Member State, pursuant to the GDPR;

“Technical and organizational security measures” means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that for the purposes of this DPA Customer is the Data Controller and Supplier is the Data Processor, and that Supplier is entitled to engage Sub-processors pursuant to the requirements set forth in Clause 5 of this DPA. Customer may permit the use of the Services to Authorized Users, including Authorized Affiliate(s) pursuant to the conditions set out in Clause 11 and 12 of this DPA, and pursuant to the Agreement.

2.2 Customer’s Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions to Epignosis for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. In addition, Customer shall have sole responsibility for the accuracy, reliability, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents, Authorized Users, or
any third parties, to whom it extends the benefits of the Services or whose Personal Data are Processed in Customer’s Use of the Services.

2.3 Epignosis’s Processing of Personal Data. a. Epignosis shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA (ii) Processing initiated by Authorized Affiliate(s), and/or Authorized User(s) in their use of the Services in accordance with the Agreement and this DPA; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. b. Customer takes full responsibility to keep the amount of Personal Data provided to Epignosis to the minimum necessary for the performance of the Services. c. Epignosis shall not be required to comply with or observe Customer’s instructions, if such instructions would violate the GDPR, CCPA, or the Data Protection Laws and Regulations. Epignosis shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR, CCPA, or the Data Protection Laws and Regulations. d. Epignosis shall process Personal Data, if required to do so by applicable law to which Epignosis is subject. In such a case, Epignosis shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Epignosis shall promptly notify Customer of any legally binding request for disclosure of Personal Data by a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

2.4 Scope of the Processing. The subject-matter of Processing of Personal Data by Epignosis is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data Processed and categories of Data Subjects involved under this DPA are further specified in Attachment 1 to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Deletion of Personal Data. For the Services, the Customer shall have the ability to request the deletion, amendment, or correction of Personal Data at any time. Following such request by Customer, Epignosis shall delete such data from its systems immediately, unless mandatory statutory law requires storage of Personal Data.

3.2 Complaints or Notices related to Personal Data. In the event Epignosis receives any official complaint, notice, or communication that relates to Processing of Personal Data for or on behalf of the Customer or either party’s compliance with Data Protection Laws and Regulations, to the extent legally permitted, Epignosis shall promptly notify Customer and, to the extent applicable, Epignosis shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Epignosis’s provision of such assistance.

3.3 Data Subject Requests. To the extent legally permitted, Epignosis shall promptly notify Customer, if Epignosis receives a request from a Data Subject to exercise the Data Subject’s rights to consent, and to withdraw the consent, right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”), and for the avoidance of doubt, similar requests as provided by the CCPA. Factoring into account the nature of the Processing, Epignosis shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Epignosis shall, upon Customer’s request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Epignosis is legally permitted to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Epignosis’s provision of such assistance.

4. EPIGNOSIS’S PERSONNEL

4.1 Confidentiality. Epignosis shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Epignosis shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Epignosis shall take commercially reasonable steps to ensure the reliability of its personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Epignosis shall ensure that its access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement, and that access is limited to those personnel that is necessary for the provision of the Services.
4.4 Data Protection Officer. Epignosis shall appoint, a Data Protection Officer, if and whereby such appointment is required by Article 37 of the GDPR. Epignosis’s personnel responsible for privacy issues may be reached at privacy@talentlms.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that

(i) Supplier is entitled to retain its Affiliates as Sub-processors. Currently Supplier engages following Affiliates as Sub-processors: a. Epignosis UK Ltd, a UK based company, having its office at 239 First Floor, Kensington High Street, London, W8 6SN, United Kingdom, tel. (+44) 20 7193 1614 (in case it is not the “Supplier”), b. the Greek Branch of Epignosis UK Ltd, established in Athens, Lykourgou 1, 10551, (+30) 211 800 6449. Customer instructs or authorizes hereby the use of these Affiliates as Sub-processors. Supplier shall inform the Customer of any intended changes to Epignosis.

(ii) Supplier may engage any third parties from time to time to process Personal Data in connection with the provision of Services. Supplier shall inform the Customer of any intention to engage any such third parties.

5.2 List of Sub-processors. Current non-Affiliate Sub-processors, are listed in Attachment 3 to this DPA, and Customer instructs or authorizes hereby the use of such Sub-processors to assist the Supplier with the performance of Supplier’s obligations under the Agreement. Supplier shall inform the Customer of any intended changes to such list. The list of non-Affiliate Sub-processors is also available in the Service administrator panel interface.

5.3 Objection Right for New Sub-processors. Customer, in order to exercise its right to object to Supplier’s use of a new Sub-processor, whether Affiliate or not, shall notify Supplier promptly in writing within ten (10) business days after receipt of Supplier’s notice about its intention to use a new Sub-processor. Personal Data shall by no means be processed by the Sub-processor against which the Customer has explicitly objected. If Supplier and Customer cannot find a mutually agreeable resolution to address the Customer’s objection within a reasonable time period, which shall not exceed thirty (30) days, the Customer may terminate the Services. The Supplier shall refund Customer any prepaid fees covering the remainder of the Service following the effective date of termination with respect to such terminated Service.

5.4 Supplier shall only engage and disclose Personal Data to Sub-processors that are parties to written agreements with each Sub-processor containing data protection obligations no less protective that the obligations of this DPA and the GDPR. Supplier agrees and warrants, upon request of the Customer, to send promptly a copy of any Sub-processor contract to the Customer, and to make available to the Data Subject upon request a copy of the DPA, or any existing Sub-processing contract, unless the DPA or contract contain commercial information, in which case it may remove such commercial information, with the exception of Attachment 2, which shall be replaced by a summary description of the security measures, in those cases where the Data Subject is unable to obtain a copy from the Customer.

5.5 Liability. The Supplier shall be liable for the acts and omissions of its Sub-processors to the same extent Supplier would be liable, if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY MEASURES, NOTIFICATIONS REGARDING PERSONAL DATA, CERTIFICATIONS AND AUDITS, RECORDS

6.1 Security Measures. Taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Epignosis shall implement appropriate organizational and technical measures to ensure a level of security, appropriate to the risk (including protection from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to Personal Data Processed under this DPA), as set forth in Attachment 2 to this DPA. Epignosis shall regularly monitor compliance with these measures. Epignosis shall not materially decrease the overall security of the Services during Customer’s subscription term. Attachment 2 may be amended from time to time, upon parties’ written agreement, to meet higher standards of safety and privacy. In such case Attachment 2 shall be replaced.

Customer agrees that after its assessment of the requirements of the Data Protection Laws and Regulations, Customer considers that the security measures set out in Attachment 2 are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of Personal Data to be protected having regard to the state of the art and the cost of their implementation.
6.2 Notifications Regarding Personal Data Breach. Epignosis has in place reasonable and appropriate security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Epignosis or its Sub-processors of which Epignosis becomes aware (hereinafter, a “Personal Data Breach”), as required under Article 33 GDPR. Epignosis shall make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as it deems necessary and reasonable in order to remediate the cause of such Personal Data Breach, to the extent that the remediation is within Epignosis’s reasonable control.

6.3 Certifications and Audits. Epignosis shall make available to the Customer all information necessary to demonstrate compliance with the obligations of Epignosis under this DPA, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer. The auditor mandated by Customer (“third party auditor”) must be independent, not a competitor of Epignosis, and composed of members in possession of the required professional qualifications bound by a duty of confidentiality. The parties agree that the audits shall be carried out in accordance with the following specifications: Customer may contact Epignosis to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Epignosis for any time expended for any such audit at Epignosis’ then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer shall inform Supplier about the scope of the audit, and Customer and Epignosis shall mutually agree upon the timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Epignosis. Customer shall promptly notify Epignosis and provide information about any actual or suspected non-compliance discovered during an audit.

Epignosis shall also and provide third-party certifications and audit results upon Customer’s written request at reasonable intervals, subject to the confidentiality obligations set forth in the Agreement. Epignosis shall make available to Customer a copy of Epignosis’s most recent third-party certifications or audit results, as applicable.

6.4 Records. Where applicable, Epignosis shall maintain a record, in electronic form, of all categories of processing activities carried out on behalf of the Customer, as per Article 30 (2) GDPR.

7. RETURN OF PERSONAL DATA, COMMUNICATION

7.1 Return of Personal Data. Epignosis shall, at the choice of the Customer, return Personal Data, to Customer in a standard and machine-readable format or delete existing copies after the end of the provision of the Services and certify to the Customer that it has done so in accordance with the procedures specified in Attachment 2 to this DPA, unless mandatory laws require storage of Personal Data. In that case Epignosis warrants that it shall guarantee the confidentiality of Personal Data and shall not Process Personal Data otherwise than exclusively for such retention, and that, in that case, Epignosis’s obligations under this DPA, as applicable, survive expiration or termination of the Agreement and completion of the Services for the full duration of such retention.

7.2 Communications. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Epignosis under this DPA and shall be entitled to transmit and receive any communication in relation to this DPA.

8. COOPERATION WITH SUPERVISORY AUTHORITY

Where applicable, Epignosis shall, upon request, cooperate with the Supervisory Authority in the performance of its tasks, as per Article 31 of the GDPR.

9. DATA PROTECTION IMPACT ASSESSMENT

Where applicable, upon Customer’s request, Epignosis shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer’s obligation under the GDPR to carry out a Data Protection Impact Assessment, according to Articles 35 and 36 of the GDPR, related to Customer’s use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Epignosis. Epignosis shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under the GDPR.

10. DATA TRANSFERS

Transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries outside of the European Economic Area are made only in accordance with the following:

i. the transfer is to a jurisdiction for which an Adequacy Decision has been issued and subject to the terms of that Adequacy Decision;
in the absence of an Adequacy Decision, the transfer is subject to the latest versions of the Standard Contractual Clauses approved by the European Commission from time to time, as published in the Official Journal of the European Union, and which themselves form part of this DPA (Attachment 4).

11. AUTHORIZED AFFILIATE(S)

11.1 Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Epignosis and each such Authorized Affiliate subject to the provisions of the Agreement and the present Clause. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

11.2 Communication. The Customer that is contracting party to the Agreement shall remain responsible for coordinating all communication with Epignosis under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s). Customer informs Epignosis of the Authorized Affiliate(s) to which Customer intends to permit the use of the Services, thereby giving Epignosis the opportunity to object, in case the requirements set out in the Definition of an Authorized Affiliate under this DPA are not met.

11.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to this DPA, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

i. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Epignosis directly by itself, the parties agree that (a) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (b) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Clause 11.3.ii below).

ii. The parties agree that the contracting party to the Agreement shall, when carrying out an on-site audit on the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Epignosis and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

12. LIABILITY

For the avoidance of doubt, Epignosis’s total liability for all claims from the Customer and all of its Authorized Affiliate(s) arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliate(s), and in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

13. LEGAL EFFECT; TERMINATION; VARIATION

This DPA shall only become legally binding between Customer and Epignosis when fully executed following the formalities steps set out in the Section “How to Execute this DPA” and will terminate when the Agreement terminates, without further action required by either party.

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

14. CONFLICT

This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control.

IN WITNESS WHEREOF, the parties have caused this Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories, whose signatures appear below, are on the date of signature duly authorized.
<table>
<thead>
<tr>
<th>CUSTOMER</th>
<th>EPIGNOSIS LLC (where applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Signature</td>
<td>Authorized Signature</td>
</tr>
<tr>
<td>Athanasios Papangelis</td>
<td>Name</td>
</tr>
<tr>
<td>Manager</td>
<td>Title</td>
</tr>
<tr>
<td>October 21, 2020</td>
<td>Date</td>
</tr>
</tbody>
</table>

| EPIGNOSIS UK LTD                                                       |                                  |
| Authorized Signature                                                   |                                  |
| Name Chris Mathiopoulos                                                 | Title Director                   |
| Date October 21, 2020                                                  |                                  |

| The GREEK BRANCH of EPIGNOSIS UK LTD                                   |                                  |
| Authorized Signature                                                   |                                  |
| Name Chris Mathiopoulos                                                 | Title Legal Representative       |
| Date October 21, 2020                                                  |                                  |
Details of the Processing

This attachment includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

Nature and Purpose of Processing

Epignosis will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Clause 8 of this DPA, Epignosis will Process Personal Data for the duration of the Agreement.

Categories of Data Subjects

Personal Data processed relates to the following categories of Data Subjects: Customer, Authorized Affiliates, Authorized Users (which may be, among others, employees, contractors or business partners of the Customer), other individuals, whose Personal Data have been stored in the Services by the Customer or the Authorized Affiliates/Clients/Users.

Type of Personal Data

Customer develops the content of the Services and determines the categories and types of Personal Data. Customer can configure the data fields through the administration panel of the Services. Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include the following categories of Personal Data:

- First name
- Last name
- Email address
- Phone number
- Time zone
- Address
- Company/branch name
- Company position
- Contract data
- Connection data
- Grades and evaluation reports
- Text, audio, video or image files
- Any Personal Data included in the content of the files uploaded by the Customer or the Authorized Users in the Services
Customer
Name:

Authorised Signature…………………………………………..

Epignosis
Epignosis LLC (where applicable)
Name: Athanasios Papangelis

Authorised Signature……………………………………………

Epignosis UK Ltd
Name: Chris Mathiopoulous

Authorised Signature……………………………………………

The Greek Branch of Epignosis UK Ltd
Name: Chris Mathiopoulous

Authorised Signature……………………………………………
Attachment 2

Description of the technical and organisational security measures implemented by the Epignosis in accordance with Article 28.3 of the GDPR, and forms part of the DPA:

1. **Data Protection Executives; Notices.** Each of the parties will designate and notify the other party of its respective Security Officer(s) responsible for the obligations set forth on this Attachment 2.

   Any notices under this Attachment should be communicated as follows:

   a. communications regarding the day-to-day obligations under this Attachment should be communicated in writing via email or other written notice to each of the Security Officer(s) (or their designees), and
   b. communications regarding any proposed changes to the terms of this Attachment should be directed as required under the notice provisions of the Agreement with copies provided to the Security Officer(s) (or their designees). No such changes will modify this Attachment or the Agreement unless agreed by the parties pursuant to the appropriate change management procedure under the Agreement.

2. **General Security Practices**

   Epignosis has implemented and shall maintain appropriate technical and organisational measures to protect Personal Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Attachment 2 for its personnel, equipment, and facilities at the Epignosis locations providing the Services.

3. **Technical and Organizational Security Measures**

3.1. **Organization of Information Security**

   a. **Security Ownership.** Epignosis has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.
   b. **Security Roles and Responsibilities.** Epignosis personnel with access to Personal Data are subject to confidentiality obligations.
   c. **Risk Management.** Epignosis performs risk assessment, including regular vulnerability scans and penetration tests.

3.2. **Human Resources Security**

   a. **General.** Epignosis informs its personnel about relevant security procedures and their respective roles. Epignosis also informs its personnel of possible consequences of breaching its security policies and procedures. Employees who violate Epignosis security policies may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of his or her contract or assignment with Epignosis.
   b. **Personal Data Visibility.** Epignosis personnel with access to Personal Data are limited to adequately trained Epignosis core team members, also adopting segregation of roles and responsibilities, data minimisation and minimum access rights to perform role principles. Epignosis employs best practices in ensuring that security threats, including malicious insider, are mitigated.

3.3. **Personnel Access Controls**

   a. **Access Policy.** An access control policy is established, documented, and reviewed based on business and information security requirements.
   b. **Access Recordkeeping.** Epignosis maintains a record of security privileges of its personnel that have access to Personal Data.
   c. **Access Authorization.**

      i. Epignosis has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to systems accessing or processing Personal Data at regular intervals based on the principle of “least privilege” and need-to-know criteria based on job role.
      ii. Epignosis maintains and updates a record of personnel authorized to access systems that contain Personal Data.
      iii. For systems that process Personal Data, Epignosis revalidates access of users.
      iv. Epignosis identifies those personnel who may grant, alter or cancel authorized access to data, systems and networks and limits them to trusted senior personnel.
v. Epignosis ensures that, each personnel having access to its systems have a single unique identifier/log-in.

vi. Epignosis maintains strict policies against any shared “generic” user identification access.

d. Least Privilege. Epignosis limits access to Personal Data to those Epignosis personnel performing the Services and, to the extent technical support is needed, its personnel performing such technical support.

f. Integrity and Confidentiality

i. Epignosis instructs its personnel to automatically lock screens and/or disable administrative sessions when leaving premises that are controlled by Epignosis or when computers are otherwise left unattended.

ii. Epignosis stores passwords in a secured and restricted way that makes them unintelligible while they are in force.

g. Authentication

i. Epignosis uses industry standard practices to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, Epignosis requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

iii. Epignosis ensures that de-activated or expired identifiers are not granted to other individuals.

iv. Epignosis maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vi. Epignosis limits access to file stores and/or systems in which passwords are stored.

3.4. Cryptography

a. Cryptographic controls policy

i. Epignosis has a policy on the use of cryptographic controls based on assessed risks.

ii. Epignosis assesses and manages the used cryptographic algorithms, hashing algorithms, etc. and deprecates and disallows usage of weak cypher suites, and mathematically insufficient block lengths and bit lengths.

iii. Epignosis cryptographic controls/policy addresses appropriate algorithm selections, key management and other core features of cryptographic implementations.

3.5. Operations Security

a. Operational Policy. Epignosis maintains policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data and to its systems and networks.

b. Data Recovery. Epignosis maintains copies of Personal Data from which Personal Data can be recovered. Epignosis has specific procedures in place governing access to these copies of Personal Data.

c. Logging and Monitoring. Epignosis maintains logs of and monitors access to administrator and operator activity and data recovery events.

3.6. Communications Security and Data Transfer

Epignosis uses standard security mechanisms and certificates for communications and data transfers.

3.7. System Acquisition, Development and Maintenance

a. Security Requirements. Epignosis has adopted security requirements for the purchase or development of information systems.

b. Development Requirements. Epignosis has policies for secure development, system engineering and support. Epignosis conducts appropriate tests for system security as part of acceptance testing processes.

3.8. Information Security Incident Management
a. **Response Process.** Epignosis maintains a record of information security breaches with a description of the breach, the consequences of the breach, the name of the reporter and to whom the breach was reported, and the procedure for recovering data.

b. **Reporting.** Epignosis will report within 48 hours to a Customer-designated response center any security incident that has resulted in a loss, misuse or unauthorized acquisition of any Personal Data.

### 3.9. Information Security Aspects of Business Continuity Management

a. **Planning.** Epignosis utilizes facilities in which Personal Data are located providing adequate emergency and contingency plans and guarantees.

b. **Data Recovery.** Epignosis’ procedures for recovering data are designed to attempt to reconstruct Personal Data in its original state from before the time it was lost or destroyed. The security measures described in this Attachment 2 are in addition to any confidentiality obligations contained in any other agreement related to the Services between Epignosis and Customer with respect to Personal Data. In the event a conflict between the terms of such other agreement and this Attachment 2, the terms of this Attachment 2 shall control.

### 4. Review and Audits

Epignosis undergoes regular audits by third parties to ensure its operations meet quality and security standards under ISO 9001 and ISO 27001 respectively. Certificates can be provided to customers upon request.

---

**Customer**

Name:

Authorised Signature:………………………………………………

---

**Epignosis LLC (where applicable)**

Name: Athanasios Papangelis

Authorised Signature:………………………………………………

---

**Epignosis UK Ltd**

Name: Chris Mathiopoulos

Authorised Signature:………………………………………………

---

**The Greek Branch of Epignosis UK Ltd**

Name: Chris Mathiopoulos

Authorised Signature:………………………………………………
Attachment 3

The list of Sub-processors approved by the Customer as of the effective date of the DPA is as set forth below; Sub-processors marked with (*) are optional and can be invoked upon Customer choice through the Service administration panel:

<table>
<thead>
<tr>
<th>Non – Affiliate Sub-processor</th>
<th>Description of Processing</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services, Inc.</td>
<td>Cloud hosting (N. Virginia USA datacenter), Storage (S3) and CDN (CloudFront)</td>
<td>Address: 1200 12th Avenue South, Suite 1200 Seattle, WA 98144, United States Phone: 1- 206-266-4064</td>
</tr>
<tr>
<td>Box, Inc.</td>
<td>Document rendering and viewing</td>
<td>Address: 64 North Row, 2nd Floor, London W1K 7LL, United Kingdom Phone: 1-888-259-5888</td>
</tr>
<tr>
<td>Stripe*</td>
<td>Payments</td>
<td>Address: 3180 18th Street, Suite 100, San Francisco, CA 94110, United States Phone: 1-650-427-9276</td>
</tr>
<tr>
<td>Paypal*</td>
<td>Payments</td>
<td>Address: 2211 North First Street San Jose, CA 95131, United States Phone: 1- 402-935-2050</td>
</tr>
<tr>
<td>Sparkpost*</td>
<td>Email gateway</td>
<td>Address: 301 Howard Street, Suite 1330, San Francisco, CA 94105, United States Phone: 1- 415-578-5222</td>
</tr>
<tr>
<td>GoToMeeting*</td>
<td>Videoconferencing</td>
<td>Address: Boston, 320 Summer Street Boston, MA 02210, United States Phone: 1-888-646-0014</td>
</tr>
<tr>
<td>Zoom.us*</td>
<td>Videoconferencing</td>
<td>Address: 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113, United States Phone: 1-888-799-9666</td>
</tr>
</tbody>
</table>

At the uses of the Services Customer has the ability, at its sole discretion, to have access and use, through the optional Service integrations, third party services, not related to the Sub-processors listed above. Epignosis assumes no responsibility for such services and may not be held liable for any such services.

**Customer**

Name:

Authorised Signature:

**Epignosis LLC (where applicable)**

Name: Athanasios Papangelis

Authorised Signature:

**Epignosis UK Ltd**

Name: Chris Mathiopoulos

Authorised Signature:
The Greek Branch of Epignosis UK Ltd

Name: Chris Mathiopoulos

Authorised Signature:

94C3D09C2DD94D8D
EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

__________________________

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

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

Name of the data exporting organisation:

Address:

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

……………………………………………………………

(the data exporter)

And

Name of the data importing organisation: Epignosis LLC

Address: 315 Montgomery Street (9th Floor) San Francisco, California CA, 94104

Tel.: (+1) 646 797 2799; e-mail: dpa@epignosishq.com

…………………………………………………………………

(the data importer)

each a “party”; together “the parties”,

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

Definitions

For the purposes of the Clauses:

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

(b) ‘the data exporter’ means the controller who transfers the personal data;

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

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

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

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

Clause 2

Details of the transfer

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

---

1 Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.
Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial
(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a

---

interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.
summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.
Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely............................
Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

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

3 This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.
Clause 12

Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Signature..................................................

On behalf of the data importer:

Name (written out in full): Athanasios Papangelis

Position: Manager

Address: 315 Montgomery Street (9th Floor) san Francisco, California CA 94104

Other information necessary in order for the contract to be binding (if any):

Signature..................................................

DocuSigned by: Athanasios Papangelis

Signature..................................................

DocuSign Envelope ID: BA711F88-9FDD-4B19-B80D-9BC1A51507C8
APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

Data importer

Epignosis LLC

Data subjects
Customer, Authorized Affiliates, Authorized Users (which may be, among others, employees, contractors or business partners of the Customer), other individuals, whose Personal Data have been stored in the Services by the Customer or the Authorized Affiliates/Clients/Users.

Categories of data
Data Exporter develops the content of the Services and determines the categories and types of Personal Data. Data Exporter can configure the data fields through the administration panel of the Services. Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled by Data Exporter in its sole discretion, and which may include the following categories of Personal Data:

- First name
- Last name
- Email address
- Phone number
- Time zone
- Address
- Company/branch name
- Company position
- Contract data
- Connection data
- Grades and evaluation reports
- Text, audio, video or image files
- Any Personal Data included in the content of the files uploaded by the Customer or the Authorized Users in the Services

Special categories of data (if appropriate)

Not applicable

Processing operations
Collection, storage, transfer, as necessary for the provision of the Services based on the Agreement

DATA EXPORTER

Name:........................................

Authorised Signature ........................

DATA IMPORTER

Name: Athanasios Papangelis

Authorised Signature ........................
APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Same as those described in Attachment 2 to this DPA.

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.