Data Processing Addendum

The parties conclude this Data Processing Addendum ("**DPA**"), which forms part of the **Agreement** between Customer and Supplier ("Epignosis"), to reflect our agreement about the Processing of Personal Data, in accordance with the requirements of Data Protection Laws and Regulations, including the GDPR. To the extent Supplier, in providing Services (TalentCards) 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 and 3 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 and Attachment 3.
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.

Data Processing Terms

Customer and Supplier hereby agree to the following provisions with respect to any Personal Data Customer discloses/transmits or in any other way announces to Supplier by using the Services.

1. DEFINITIONS

"Adequacy Decision" means a European Commission Decision that a third country or an international organization ensures an adequate level of data protection.

"Affiliate" means, with respect to any entity, any other entity Controlling, Controlled by or under common Control with such entity, for only so long as such Control exists;

"Control" means the direct or indirect ownership of more than 50% of the voting capital or similar right of ownership of an entity, or the legal power to direct or cause the direction of the general management and policies

of that entity, whether through the ownership of voting capital, by contract or otherwise. Control and Controlling shall be construed accordingly;

"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. For purposes of this DPA, Customer is the Data Controller;

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, as defined in the GDPR. For the purposes of this DPA, Supplier is the Data Processor;

"Data Protection Laws and Regulations" means all mandatory laws and regulations, including laws and regulations (including the Privacy Shield) of the European Union, the European Economic Area and their member states, the latter to the extent applicable to the Processing of Personal Data under the Agreement, including the requirements of the Article 28 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, and repealing Directive 95/46/EC (General Data Protection Regulation), which comes into force on 25th May 2018, or any amendment or replacement thereof;

"Data Subject" means the individual to whom Personal Data relates as defined in the GDPR;

"Epignosis" means the Epignosis entity, which is a party to this DPA, being Epignosis LLC, a US based company, having its registered office at 315 Montgomery Street (9th Floor) San Francisco, California CA 94104 USA, (+1) 646 797 2799 or Epignosis UK Ltd, a UK based company, having its registered office at Crown House, 72 Hammersmith Rd, London UK, (+44) 20 7193 1614.

"Epignosis Group" means Epignosis and its Affiliates engaged in the Processing of Personal Data with regard to the Management, Delivery and Administration of the Services.

"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 disclosed, transmitted or in any other way announced to Supplier for the use of the Services within the Agreement, from which that person is identified or identifiable, as defined in the GDPR;

"Privacy Shield" means Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (C(2016) 4176 final);

"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;

"Supplier's Representative" means a natural or legal person established in the European Union who is designated by the Supplier and represents the Supplier with regard to its respective obligations under the GDPR, as applicable.

"Sub-processor" means any non-Supplier or Supplier Affiliate Data Processor, engaged by the Supplier, who agrees to receive from the Supplier or from any other Sub-processor of the 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 Customer's Processing of Personal Data. Customer shall, in its use of the Services, comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions to the Supplier for the Processing of Personal Data must comply with Data Protection Laws and Regulations. In addition, Customer shall have sole responsibility for the accuracy, reliability, integrity, 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 or third parties to whom it extends the benefits of the Services.

It is expressly stated that the Customer agrees and warrants:

(a) that the Processing of Personal Data shall be carried out in accordance with the relevant provisions of the Data Protection Laws and Regulations, (and, where applicable, has been notified to the relevant authorities of the Member State where the Customer is established) and does not violate the relevant provisions of that State;

(b) that it shall instruct throughout the duration of the Personal Data Processing the Supplier to process the Personal Data only on the Customer's behalf and in accordance with the Data Protection Laws and Regulations;

(c) that the Supplier shall provide sufficient guarantees in respect of the technical and organizational security measures specified in Article 7 of the DPA and Attachment 2 to this DPA;

(d) that after assessment of the requirements of the Data Protection Laws and Regulations, the security measures are appropriate to protect 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, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected having regard to the state of the art and the cost of their implementation;

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

(f) that, if Processing involves special categories of data, the Data Subject has been informed and explicit consent has been acquired;

(g) to forward any notification received from the Supplier or any Sub-processor pursuant to Article 7.2 of this DPA to the Supervisory Authority;

(h) to make available to the Data Subjects upon request a copy of the DPA, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any Sub-processing contract, unless the DPA or the Sub-processing contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of Sub-processing, Processing is carried out in accordance with the Data Protection Laws and Regulation, providing at least the same level of protection for the personal data and the rights of Data Subject as the Supplier under the DPA;

(j) that it shall meet its record keeping obligations under Article 30 of the GDPR;

(k) that it shall designate in writing a representative in the Union, if and whereby such appointment is required under the GDPR;

(l) that it shall appoint and designate a Data Protection Officer, if and whereby such appointment is required under the GDPR;

(m) that it shall notify any Personal Data Breach, as required by the GDPR;

(n) that it shall ensure compliance with Article 2.1.

2.2 Supplier's Processing of Personal Data. Supplier 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; (ii) Processing initiated by Authorized Users in their use of the Service; 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. Customer takes full responsibility to keep the amount of Personal Data provided to Supplier to the minimum necessary for the performance of the Services. The Supplier shall not be required to comply with or observe Customer's instructions, if such instructions would violate the GDPR or the Data Protection Laws and Regulations.

3. SCOPE OF PROCESSING

3.1 Scope. The subject-matter of Processing of Personal Data by the Supplier 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 and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 to this DPA.

4. RIGHTS OF DATA SUBJECTS

4.1 Deletion of Personal Data. For the Services, the Customer shall have the ability, upon termination of this DPA, to request the deletion of Personal Data. Following such deletion request by Customer, Supplier shall delete such data from its systems as soon as reasonably practicable, unless mandatory statutory law requires storage of Personal Data.

4.2 Data Subject Requests. Supplier shall, to the extent legally permitted, promptly notify Customer, if it receives a request from a Data Subject for access to, correction, amendment or deletion of such Data Subject's Personal Data. Supplier shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. The Supplier shall provide Customer with commercially-reasonable cooperation and assistance in relation to handling a Data Subject's request for access to that person's Personal Data. To the extent Customer, in its use of the Service, does not have the ability to access, correct, block or delete Personal Data or object to the Processing, the Supplier shall comply with any commercially-reasonable request by Customer to facilitate such actions to the extent Supplier is legally permitted to do so. Customer shall be responsible for any costs arising from Supplier's provision of such assistance.

4.3 Complaints or Notices related to Personal Data. In the event Supplier 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, Supplier shall promptly notify Customer and, to the extent applicable, Supplier 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 Supplier's provision of such assistance.

4.4 Post-GDPR Data Subject Requests. Effective from 25 May 2018, the following wording will replace the immediately-preceding subsections 4.2 and 4.3 in their entirety: To the extent legally permitted, Supplier shall promptly notify Customer, if Supplier receives a request from a Data Subject to exercise the Data Subject's right 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"). Factoring into account the nature of the Processing, Supplier shall assist Customer by appropriate organizational and technical measures 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 Service, does not have the ability to address a Data Subject Request, Supplier shall, upon Customer's request, provide

commercially-reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Supplier is legally authorized 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 Supplier's provision of such assistance.

The Supplier ensures that the Service has incorporated technical and organizational measures for the accommodation of Customer's obligations to facilitate the exercise of the Data Subject's rights under the GDPR.

4.5 Right to compensation and liability.

4.5.1 Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the Customer or the Supplier for the damage suffered.

4.5.2. The Customer shall be liable for the damage caused by Processing, which infringes the GDPR. The Supplier shall be liable for the damage caused by Processing, only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Customer.

4.5.3. Customer or Supplier shall be exempt from liability under sub paragraph 2, if it proves that it is not in any way responsible for the event giving rise to the damage.

4.5.4. Where both Customer and Supplier are, under sub paragraphs 2 and 3, responsible for any damage caused by Processing, Customer or Supplier shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject.

4.5.5. Where Customer or Supplier has, in accordance with sub paragraph 4, paid full compensation for the damage suffered, Customer or Supplier shall be entitled to claim back from the other party that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in sub paragraph 2.

4.5.6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State, where the Customer or the Supplier has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State, where the Data Subject has his or her habitual residence, unless the Customer is a public authority of a Member State acting in the exercise of its public powers.

5. SUPPLIER'S PERSONNEL

5.1 Confidentiality. The Supplier shall ensure that Epignosis Group 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. The Supplier shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

5.2 Reliability. The Supplier shall take commercially-reasonable steps to ensure the reliability of Epignosis Group personnel engaged in the Processing of Personal Data.

5.3 Limitation of Access. The Supplier shall ensure that Supplier's access to Personal Data is limited to those personnel of Epignosis Group assisting in the provision of the Services in accordance with the Agreement.

5.4 Data Protection Officer. Effective from 25 May 2018, Members of Epignosis Group shall have appointed, or shall appoint, a Data Protection Officer, if and whereby such appointment is required by Article 37 of the GDPR. Any such appointed person and/or Supplier and Supplier's Affiliate personnel responsible for privacy issues, including but not limited to giving notice of the discrepancy to the Supervisory Authority, if the discrepancy has resulted in the unauthorized disclosure of Personal Data, may be reached at privacy@talentcards.io. Additionally, the Supplier shall publish the contact details of the Data Protection Officer/s and communicate such contact details to the Supervisory Authority.

6. SUB-PROCESSORS

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

(i) the Supplier is entitled to retain its Affiliates as Sub-processors. Currently Epignosis Group members are Epignosis LLC, and Epignosis UK Ltd, with its Greek Branch established in Athens, Lykourgou Str, 1, 10551, (+30) 211 800 6449. Supplier shall inform the Customer of any intended changes to Epignosis Group.

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

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

6.3 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 the Supplier promptly in writing within ten (10) business days after receipt of Supplier's notice about its intention to use a new Sub-processor. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, the Supplier shall use reasonable efforts to make available to Customer a change in the Services or recommend a commercially-reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If the Supplier is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the Services, which cannot be provided by the Supplier without the use of the objected-to new Sub-processor by providing written notice to the Supplier. 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.

6.4 Any Member of Epignosis Group shall only engage and disclose Personal Data to Sub-processors that are parties to written agreements with each Subprocessor containing data protection obligations no less protective that the obligations of this DPA and the GDPR. The Supplier agrees and warrants, upon request of the Customer, to send promptly a copy of any Sub-processor contract (concluded by any member of Epignosis Group) 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.

6.5 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.

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

7.1 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, the Supplier shall implement appropriate organizational and technical measures to ensure a level of security, appropriate to the risk (including risks that are presented by Processing, in particular from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed), including inter alia:

(a) the encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical and technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Such technical and organizational security measures are further described in Attachment 2 to this DPA. The Supplier shall not materially decrease the overall security of the Services during Customer's subscription term. Supplier and Customer shall take appropriate measures to ensure that any natural person acting under the authority of the Supplier or the Sub-processors or the Customer who has access to Personal Data does not process them except on instructions from the Customer, unless he or she is required to do so by Union or Member State Law.

7.2 Notifications Regarding Personal Data Breach. The Supplier 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 the Supplier or its Sub-processors of which the Supplier becomes aware (hereinafter, a "Personal Data Breach"), as required to assist the Customer in ensuring compliance:

(a) with its obligations to notify the Supervisory Authority, pursuant to Article 33 paragraph 1 and 3 of the GDPR,

(b) with its obligations to communicate the Personal Data Breach to the Data Subject involved, pursuant Article 34 of the GDPR,

(c) as well as with its documentation obligation regarding the facts relating to the Personal Data Breach, its effects, and the remedial action taken, pursuant Article 33 paragraph 5 of the GDPR.

The Supplier 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 a Personal Data Breach, to the extent that the remediation is within Supplier's reasonable control.

7.3 Certifications and Audits. The Supplier shall make available to the Customer all information necessary to demonstrate compliance with the obligations of the Supplier under this DPA, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer. At the request of the Customer, the Supplier shall submit its data processing facilities for audit of the Processing, which shall be carried out by the Customer 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 Customer, where applicable, in agreement with the Supervisory Authority. The parties agree that the audits shall be carried out in accordance with the following specifications: Customer may contact Supplier to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Supplier for any time expended for any such audit at the Supplier's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and the Supplier shall mutually agree upon the scope, 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 the Supplier. Customer shall promptly notify the Supplier and provide information about any actual or suspected non-compliance discovered during an audit.

The Supplier shall also allow 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. The Supplier shall make available to Customer a copy of Supplier's most recent third-party certifications or audit results, as applicable.

7.4 Records. The Supplier, and the Supplier's Representative, as applicable, shall maintain, and make available on request to the Supervisory Authority, a record, in electronic form, of all categories of processing activities carried out on behalf of the Customer, containing:

(d) the name and contact details of the Supplier, the Supplier's Representative, as applicable, the Sub-processors and of the Customer, and the Data Protection Officer;

(e) the categories of processing carried out on behalf of the Customer;

(f) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49 (1) of the GDPR, the documentation of suitable safeguards;

(g) where possible, a general description of the technical and organizational security measures referred to in Article 32 (1) of the GDPR, described in Attachment 2 of this DPA.

8. RETURN OF PERSONAL DATA, COMMUNICATION

8.1 Return of Personal Data. The Supplier shall return Personal Data, to Customer and, to the extent allowed by applicable law, 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 the retention of the Data is requested from the Supplier according to mandatory statutory laws. In that case the Supplier warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

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

9. COOPERATION WITH SUPERVISORY AUTHORITY

Customer, Supplier, and the Supplier's Representative, as applicable, shall cooperate, on request, with the Supervisory Authority in the performance of its tasks.

10. ADDITIONAL TERMS FOR TRANSFER OF PERSONAL DATA FROM THE EEA

Any transfer of Personal Data (directly or via onward transfer) to a third country or to an international organization shall take place only if, subject to the other provisions of the GDPR, the conditions laid down in Chapter V of the GDPR are complied with by the Sub-processors.

The Supplier warrants that Epignosis Group members and Sub-processors are self-certified to and comply with the Privacy Shield, where applicable, and/or with any other Adequacy Decision, and shall maintain their self-certification to and compliance with the Privacy Shield, and/or any other Adequacy Decision with respect to the Processing of Personal Data in the framework of the Services.

11. GDPR

Effective from 25 May 2018, the Supplier shall Process Personal Data in accordance with the GDPR requirements directly applicable to the Supplier's provision of its Services.

12. DATA PROTECTION IMPACT ASSESSMENT

Effective from 25 May 2018, upon Customer's request, the Supplier shall provide Customer with reasonable cooperation and assistance needed to fulfil 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 Supplier. The Supplier 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.

13. LEGAL EFFECT; TERMINATION; VARIATION

This DPA shall only become legally binding between Customer and the Supplier when fully executed following the formalities steps set out in the Section “How to Execute this DPA” and will terminate when the Main 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.

CUSTOMER

Authorised Signature……..

Name:

Title:

Date:

EPIGNOSIS LLC

Authorised Signature……..

Name: Athanasios Papangelis

Title: Co-CEO and CTO

Date:

EPIGNOSIS UK LtD

Authorised Signature……

Name: Athanasios Papangelis

Title: Co-CEO and CTO

Date:

The GREEK BRANCH of EPIGNOSIS UK LtD

Authorised Signature……

Name: Athanasios Papangelis

Title: Co-CEO and CTO

Date:

Attachment 1

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

Supplier 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 Section 8 of the DPA, Supplier will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Unless otherwise agreed upon in writing, the Supplier shall return Personal Data, to Customer and, to the extent allowed by applicable law, 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 the retention of the Data is requested from the Supplier according to mandatory statutory laws. In that case the Supplier warrants that it shall guarantee the confidentiality of the Personal Data and shall not actively process Personal Data transferred anymore.

Categories of Data Subjects

Personal Data processed relates to the following categories of Data Subjects: Customer, 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 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 LLC

Name: Athanasios Papangelis

Authorised Signature……..

Epignosis UK Ltd

Name: Athanasios Papangelis

Authorised Signature……

The Greek Branch of Epignosis UK Ltd

Name: Athanasios Papangelis

Authorised Signature……

Attachment 2

Description of the technical and organisational security measures implemented by the Supplier 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 Data Protection Executive(s) responsible for the obligations set forth on this Attachment 2.

   Any notices under this Attachment or the underlying Agreement should be communicated as follows:

   a. communications regarding the day-to-day obligations should be communicated in writing via email or other written notice to each of the Data Protection Executives (or their designees), and

   b. communications regarding any proposed changes to the terms of this Attachment or the terms of a party's Personal Data obligations under the Agreement should be directed as required under the notice provisions of the Agreement with copies provided to the Data Protection Executives (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**

   2.1. Epignosis Group 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 Group locations providing the Services.

3. **Technical and Organizational Security Measures**

   3.1. Organization of Information Security

   a. **Security Ownership.** Epignosis Group has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

   b. **Security Roles and Responsibilities.** Epignosis Group personnel with access to Personal Data are subject to confidentiality obligations.

   c. **Risk Management.** Epignosis Group performs risk assessment.

   3.2. Human Resources Security

   a. **General**. Epignosis Group informs its personnel about relevant security procedures and their respective roles. Epignosis Group also informs its personnel of possible consequences of breaching its security policies and procedures. Employees who violate Epignosis Group 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 Group.

   b. **Personal Data Visibility.** Epignosis Group personnel with access to Personal Data are limited to adequately trained Supplier core team members, also adopting segregation of roles and responsibilities, data minimisation and minimum access rights to perform role principles. Supplier 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 Group maintains a record of security privileges of its personnel that have access to Personal Data.

   c. **Access Authorization.**

i. Epignosis Group 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 Group maintains and updates a record of personnel authorized to access systems that contain Personal Data.

iii. For systems that process Personal Data, Epignosis Group revalidates access of users.

iv. Epignosis Group 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 Group ensures that, each personnel having access to its systems have a single unique identifier/log-in.

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

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

e. **Integrity and Confidentiality**

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

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

f. **Authentication**

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

ii. Where authentication mechanisms are based on passwords, Epignosis Group 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 Group ensures that de-activated or expired identifiers are not granted to other individuals.

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

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

3.4. Cryptography

a. **Cryptographic controls policy**

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

ii. Epignosis Group 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 Group’s cryptographic controls/policy addresses appropriate algorithm selections, key management and other core features of cryptographic implementations.

3.5. Operations Security

a. **Operational Policy.** Epignosis Group 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 Group maintains copies of Personal Data from which Personal Data can be recovered. Epignosis Group has specific procedures in place governing access to these copies of Personal Data.

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

3.6. Communications Security and Data Transfer

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

3.7. System Acquisition, Development and Maintenance

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

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

3.8. Information Security Incident Management

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

b. **Data Recovery.** Epignosis Group's 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.

4. 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.

Customer

Name:

Authorised Signature……..

Epignosis LLC

Name: Athanasios Papangelis

Authorised Signature……..

Epignosis UK Ltd

Name: Athanasios Papangelis

Authorised Signature……

The Greek Branch of Epignosis UK Ltd

Name: Athanasios Papangelis

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:

Non – Affiliate Sub-processor	Description of Processing	Contact Information
Rackspace, Inc.	Cloud hosting (USA Chicago datacenter)	**Address:** 1 Fanatical Place, City of Windcrest San Antonio, TX 78218, United States **Phone:** 1-800-961-4454
Amazon Web Services, Inc.	Storage (S3) and CDN (CloudFront)	**Address:** 1200 12th Avenue South, Suite 1200 Seattle, WA 98144, United States **Phone:** 1- 206-266-4064
Stripe*	Payments	**Address:** 3180 18th Street, Suite 100, San Francisco, CA 94110, United States **Phone:** 1-650-427-9276
Sparkpost	Email gateway	**Address:** 301 Howard Street, Suite 1330, San Francisco, CA 94105, United States **Phone:** 1- 415-578-5222
Twilio*	SMS Gateway	**Address:** 375 Beale Street, Suite 300, San Francisco, CA 94105, United States

Customer

Name:

Authorised Signature……..

Epignosis LLC

Name: Athanasios Papangelis

Authorised Signature……..

Epignosis UK Ltd

Name: Athanasios Papangelis

Authorised Signature……

The Greek Branch of Epignosis UK Ltd

Name: Athanasios Papangelis

Authorised Signature……