REWARDFUL DATA PROCESSING AGREEMENT

This Data Processing Agreement (***"DPA"***), applies to the Agreement between **REWARDFUL INC.** (***"Rewardful"***), and any customer of Rewardful (***"Customer"***) (collectively referred to as the ***"Parties"***), sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Rewardful to Customer (and no other person) pursuant to the agreement entered into between the Parties whereby the Customer subscribed for Rewardful's services (the ***"Agreement"***).

I. Definitions

(A) ***"Applicable Law"*** means all applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive"), as replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications.

(B) ***"Data Controller"*** means a person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

(C) ***"Data Processor"*** means a person who Processes Personal Data on behalf of the Data Controller.

(D) ***"Data Security Measures"*** means technical and organisational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorised access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.

(E) ***"Data Subject"*** means an identified or identifiable natural person to which the Personal Data pertain.

(F) ***"Instructions"*** means this DPA and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

(G) ***"Personal Data"*** means any information relating to an identified or identifiable natural person Processed by Rewardful in accordance with Customer's Instructions pursuant to this DPA; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(H) ***"Personal Data Breach"*** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

(I) ***"Process", "Processed",*** or ***"Processing"*** means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(J) ***"Services"*** means the services offered by Rewardful and subscribed for by Customer under the Master Agreement.

(K) ***"Sub-Processor"*** means the entity engaged by the Data Processor or any further Sub-Processor to Process Personal Data on behalf and under the authority of the Data Controller.

II. Roles and Responsibilities of the Parties

(A) The Parties acknowledge and agree that Customer is acting as a Data Controller, and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this DPA, and Rewardful is acting as a Data Processor on behalf and under the Instructions of Customer.

(B) Customer acknowledges that it shall not make Personal Data available to Rewardful other than to the extent strictly required in relation to the Services

(C) Any Personal Data will at all times be and remain the sole property of Customer and Rewardful will not have or obtain any rights therein.

III. Obligation of Rewardful

Rewardful agrees and warrants to:

(A) Process Personal Data disclosed to it by Customer only on behalf of and in accordance with the Instructions of the Data Controller and to the extent strictly necessary to provide the Services (as defined in the Agreement), unless Rewardful is otherwise required by Applicable Law, in which case Rewardful shall inform Customer of that legal requirement before

Processing the Personal Data, unless informing the Customer is prohibited by law on important grounds of public interest. Rewardful shall immediately inform Customer if, in Rewardful's opinion, an Instruction provided infringes Applicable Law.
(B) Ensure that any person authorised by Rewardful to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Data Controller.
(C) Rewardful stores and Processes all data, including Personal Data, in the US and/or Canada. Rewardful has and shall continue to enter into any written agreements as are necessary (in its reasonable determination) to comply with Applicable Law concerning any cross-border transfer of Personal Data, whether to or from Rewardful.
(D) Inform Customer promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by the Customer in writing to do so. Taking into account the nature of the Processing of Personal Data, Rewardful shall assist Customer, by appropriate technical and organisational measures, insofar as possible, in fulfilling Customer's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.
(E) Notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer shall have the right to defend such action in lieu of and on behalf of Rewardful. Customer may, if it so chooses, seek a protective order. Rewardful shall reasonably cooperate with Customer in such defense.
(F) Provide reasonable assistance to Customer at Customer's cost, in complying with Customer's obligations under Applicable Law available.
(G) Maintain internal record(s) of Processing activities, copies of which shall be provided to Customer by Rewardful or to supervisory authorities upon request.
(H) Comply with the Standard Contractual Clauses as set out at Exhibit 1 where there is a transfer of personal data from a EU member state to a country outside of the EU member state where (i) it is transferred to a jurisdiction which is not recognised as having adequate protections in place by the European Commission; and (ii) is not otherwise subject to an alternate regime recognised by the European Commission as providing sufficient safeguards, such as through the Privacy Shield framework.

IV. Sub-Processing

(A) Rewardful shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless Rewardful has entered into a written agreement with each such third party that imposes obligations on the third party that are similar to those imposed on Rewardful under this DPA. Rewardful shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data. Rewardful shall inform Customer of the identity of each such third party and shall notify Customer if Rewardful intends to use an alternate third party provider for such purposes in advance. Customer shall have the right to object to the identity of any such alternate third party provider and, in the event that Rewardful continues to engage such alternate third party provider despite such objection, to terminate this Agreement and the Master Agreement immediately on notice without any further liability to Rewardful.

V. Compliance with Applicable Laws

(A) Each party covenants and undertakes to the other that it shall comply with all Applicable Laws in the use of the Services.
(B) Without limiting the above, (i) Customer is responsible for ensuring that it has a lawful basis for the processing of Personal Information in the manner contemplated by this Agreement, and has adequate record of such basis (whether directly or through another third party provider); and (ii) Rewardful is not responsible for determining the requirements of laws applicable to Customer's business or that Rewardful's provision of the Services meet the requirements of such laws. As between the parties, Customer is responsible for the lawfulness of the Processing of the Customer Personal Data. Customer will not use the Services in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.
(C) Subject to the terms of the Agreement, Customer may claim from Rewardful amounts paid to a Data Subject for a violation of their Data Subject rights caused by Rewardful's breach of its obligations under GDPR.

VI. Data Security

(A) Rewardful shall develop, maintain and implement a comprehensive written information security program that complies with Applicable Law and good industry practice. Rewardful's information security program shall include appropriate

administrative, technical, physical, organisational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:
a) The encryption of the 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 the Personal Data in a timely manner in the event of a physical or technical incident; and
d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures adopted pursuant to this provision for ensuring the security of the Processing.
(B) Rewardful shall supervise Rewardful personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. Rewardful shall provide training, as appropriate, to all Rewardful personnel who have access to Personal Data.
(C) Promptly (and in any event within 90 days) following the expiration or earlier termination of the Master Agreement, Rewardful shall return to Customer or its designee, if so requested during such period, or if not so requested securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Rewardful's, its affiliates' or their respective subcontractors' possession, custody or control. In the event applicable law does not permit Rewardful to comply with the delivery or destruction of the Personal Data, Rewardful warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this DPA.

VII. Data Breach Notification
(A) Rewardful shall promptly inform Customer in writing of any Personal Data Breach of which Rewardful becomes aware. The notification to Customer shall include all available information regarding such Personal Data Breach, including information on:
a) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;
b) The likely consequences of the Personal Data Breach; and
c) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
Rewardful shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. Rewardful shall provide such assistance as required to enable Customer to satisfy Customer's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR.

VIII. Audit
Rewardful shall on written request (but not more than once per year, other than in the event of a breach) make available to Customer all information necessary to demonstrate compliance with the obligations set forth in this DPA and, at the Customer's expense, allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer not more than once per year, other than in the event of a breach. Upon prior written request by Customer (but not more than once per year, other than in the event of a breach) (provided that it shall be not more than once per year other than in the event of a breach, Rewardful agrees to cooperate and, within reasonable time, provide Customer with: (a) audit reports (if any) and all information necessary to demonstrate Rewardful's compliance with the obligations laid down in this DPA; and (b) confirmation that no audit, if conducted, has revealed any material vulnerability in Rewardful's systems, or to the extent that any such vulnerability was detected, that Rewardful has fully remedied such vulnerability.

IX. Governing Law
This DPA shall be governed by the laws of the jurisdiction specified in the Agreement.

EXHIBIT 1 – Standard Contractual Clauses

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 ([1]);

(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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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.

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 sub-processor 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 sub- processor 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor 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:

(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 sub-processing, 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 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of

the data importer, or any sub-processor, 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 primary agreement to which it is appended.

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 Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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.

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 sub-processor 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 sub-processor 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.

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

The data exporter is the Data Controller.

Data importer

The data importer is Rewardful.

Data subjects

Customer may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Customer's contacts and other end users including Customer's employees, contractors and collaborators who are authorised to use the Service.
- Prospects, customers, business partners and vendors of the Customer as required to provide the Service.
- Individuals, organizations, and companies who act as promoters (i.e. affiliates) for the Customer.

Categories of data

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Contact information (i.e. company, email, phone, physical business address)
- Technical and network information (i.e. IP address, web browser and device metadata)
- Localization preferences (i.e. timezone and language)
- Sales/transaction information (i.e. details related to referral sales), excluding sensitive payment details
- Any other Personal Data submitted by, sent to, or received by Customer, or Customer's end users, via the Service.

Special categories of data

The parties do not anticipate the transfer of special categories of data.

Processing operations

The objective of Processing of Personal Data by data importer is the performance of Services pursuant to the Rewardful Terms of Service and Privacy Policy.

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide, maintain and improve Services provided to Customer; and/or
- Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

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):

- Network data is encrypted in transit using HTTPS/SSL (SHA-256 with RSA Encryption)
- Data housed in Postgres is encrypted at rest with AES-256, block-level storage encryption.
- Additionally, sensitive data (passwords, API keys, etc) is encrypted at the database layer.
- Cookies that store sensitive data (i.e. session authentication) are encrypted and use the "Secure" and "HttpOnly" attributes to prevent XSS attacks.
- The web application uses the Ruby on Rails framework, which includes many security features to prevent attacks, including XSS, CSRF, SQL injection, session fixation, etc. For full details, please refer to https://guides.rubyonrails.org/security.html
- Application-level firewall to prevent DDoS and brute-force attacks.
- Users of the Service are required to use a strong password and/or API key. Users must provide their password to make changes to account information. Users must confirm email addresses when signing up for the Service and when making changes to their email address. Password reset links are only sent to confirmed email addresses, can be used only once, and expire after 24 hours.
- Employees of data importer use strong passwords, two-factor authentication (where possible) and only access Personal Data on a need-to-know basis as required to provide Service.
- Personal Data that is no longer required by the Service is automatically purged after a period of time wherever possible.

All technical infrastructure is hosted on Heroku. The Heroku security policy covers:

- Vulnerability Reporting
- Security Assessments and Compliance
- Penetration Testing and Vulnerability Assessments
- Environmental Safeguards
- Network Security
- Data Security
- System Security
- Vulnerability Management
- Backups
- Disaster Recovery

For full details, please refer to https://www.heroku.com/policy/security

Last updated October 5, 2020