TREASURE DATA

Updated: December 28, 2022

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the terms of service, master service agreement or other agreement that governs the purchase of Services between Treasure Data, Inc. and the counterparty thereunder ("**Customer**") and that references this DPA ("**Service Agreement**"). This DPA governs the Parties' responsibilities with regard to the Processing of Personal Data by Treasure Data for Customer in connection with the provision of the Services. Customer and Treasure Data are hereunder jointly referred to as the "**Parties**", and each separately as a "**Party**".

1. DEFINITIONS

For the purposes of this DPA, the following capitalized words are ascribed the following meanings. All capitalized terms not defined in this DPA shall have the meaning ascribed to them in the Service Agreement.

1.1 "**Agreement**" means the Service Agreement together with this DPA.

1.2 **"CCPA"** means the California Consumer Privacy Act 2018, codified at Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 ("**CPRA**") and implementing regulations, all of the foregoing as amended, superseded or replaced from time to time.

1.3 "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.4 "**Collected Data**" has the meaning ascribed to it in the Service Agreement.

1.5 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.6 **"Data Subject Request"** has the meaning ascribed to it under Clause 4.2.

1.7 "**Data Protection Legislation**" means all laws and regulations relating to the protection of personal data and privacy of individuals (as amended, superseded or replaced from time to time), including without limitation the CCPA, the GDPR, the European Directive 2002/58/EC (as amended by Directive 2009/136/EC) and implementing national legislation, the Personal Information Protection and Electronic Documents Act of Canada and the Act on the Protection of Personal Information of Japan.

1.8 "**Documented Instructions**" has the meaning ascribed to it under Clause 3.2.

1.9 "**DPA**" has the meaning ascribed to it above.

1.10 "**EEA**" means the European Economic Area.

1.11 **"EU C-to-P Transfer Clauses"** means Module Two (Controller-to-Processor) of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as completed pursuant to Schedule 3 – Part 1 and Part 2 of this DPA.

1.12 **"EU Data Protection Legislation"** means the GDPR, the UK GDPR and the FDPA.

1.13 "**EU P-to-P Transfer Clauses"** means Module Three (Processor-to-Processor) of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.14 **"FDPA"** means the Federal Data Protection Act of 19 June 1992 (Switzerland) and its respective ordinances, each as amended, superseded or replaced from time to time.

1.15 "**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 (General Data Protection Regulation), as amended, superseded or replaced from time to time.

1.16 "**Personal Data**" means any information relating to an identified or identifiable natural person where such information is Collected Data.

1.17 "**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Treasure Data under the Agreement.

1.18 "**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, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.19 "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Personal Data protected under the GDPR from the EEA to a country outside the EEA which is not subject to an adequacy determination by the European Commission and that would not be lawful under the GDPR in the absence of the protection for the transferred Personal Data provided by the EU C-to-P Transfer Clauses; (ii) where the UK GDPR applies, a transfer of Personal Data protected under the UK GDPR from the UK to any other country which is not subject to an adequacy determination by the competent UK authority and that would not be lawful under the UK GDPR in the absence of the protection for the transferred Personal Data provided by the UK Addendum; and (iii) where the FDPA applies, a transfer of Personal Data protected under the FDPA from Switzerland to any other country which is not subject to an adequacy determination by the competent Swiss authority and that would not be lawful under the FDPA in the absence of the protection for the transferred Personal Data provided by the EU C-to-P Transfer Clauses, as adapted pursuant to Schedule 3 – Part 3.

1.20 "**Services"** means the cloud-based Service and any ancillary services (such as Customer Support or Professional Services) provided by Treasure Data under the Service Agreement.

1.21 **"Service Agreement"** has the meaning ascribed to it above.

1.22 "**Processor**" means the entity which Processes Personal Data on behalf of a Controller.

1.23 **"Standard Contractual Clauses"** means any of the transfer mechanisms detailed at Clause 7.2, letters a), b) and c).

1.24 "**Sub-processor**" means a third party that Treasure Data or a Treasure Data Subsidiary engages for the Processing of Personal Data on behalf of Customer.

1.25 "**Supervisory Authority**" means an independent public authority charged with overseeing the compliance with Data Protection Legislation.

1.26 **"Treasure Data Subsidiary"** means any company the majority of whose voting shares is now or hereafter owned or controlled, directly or indirectly, by Treasure Data. A company shall be a Subsidiary only for the period during which such control exists.

1.27 **"UK"** means the United Kingdom.

1.28 **"UK Addendum"** means the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018, Version B1.0, as completed pursuant to Schedule 3 – Part 4 of this DPA.

1.29 **"UK GDPR"** means the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, as amended, superseded or replaced from time to time.

2. ROLES OF THE PARTIES

2.1 Customer shall, in its use of the Services, Process Personal Data at all times in accordance with the requirements of the applicable Data Protection Legislation and in accordance with the Agreement.

2.2 As between Customer and Treasure Data, Customer has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Personal Data were acquired.

2.3 Customer represents and warrants to Treasure Data that: (a) it is the Controller of the Personal Data; (b) If Customer is not the only Controller of the Personal Data, any third party who is a Controller of the Personal Data agrees to the Processing by Treasure Data of the Personal Data pursuant to the Agreement and the Documented Instructions provided to Treasure Data pursuant to the Agreement.

2.4 Customer acts as a single point of contact and is responsible for obtaining any relevant authorizations, consents and permissions for the Processing of Personal Data in accordance with the Agreement. Where authorizations, consent, instructions or permissions are provided by Customer, these are provided not only on behalf of Customer but also on behalf of all relevant Controllers of the Personal Data. Where Treasure Data informs or gives notice to Customer, it is Customer's responsibility to forward such information and notices to any relevant Controller(s) (as applicable) without undue delay.

3. CUSTOMER'S INSTRUCTIONS AND CONFIDENTIALITY

3.1 The subject matter of the Processing of Personal Data by Treasure Data in the performance of the Services pursuant to the Service Agreement, the duration, the nature and purpose of such Processing, the types of Personal Data Processed under the Service Agreement and relevant categories of Data Subjects are specified in Schedule 1 to this DPA.

3.2 The Parties agree that this DPA and the Service Agreement and the instructions provided via configuration or other tools made available by Treasure Data under the Service Agreement (such as APIs or SDKs) constitute Customer's documented instructions regarding Treasure Data's Processing of Personal Data under the Agreement ("**Documented Instructions**"). The Documented Instructions shall comply with applicable Data Protection Legislation and any other laws and regulations applicable to Customer.

3.3 If, in Treasure Data's opinion, any Documented Instruction infringes Data Protection Legislation, Treasure Data will immediately inform Customer. For the avoidance of doubt, this Clause 3.3 does not imply an obligation on Treasure Data to conduct any legal review of any Documented Instruction and any communication or information provided by Treasure Data to Customer pursuant to this Clause 3.3 is not and shall not be deemed to be legal advice.

3.4 Treasure Data shall process Personal Data in accordance with the Documented Instructions, unless otherwise required by law to which Treasure Data is subject. In such a case, Treasure Data shall inform Customer of such legal requirement before Processing, unless the law prohibits such disclosure.

3.5 Any instruction related to the Processing of Personal Data additional to the Documented Instructions require prior written agreement between the Parties, including agreement on any additional fees payable by Customer to Treasure Data for carrying out such instruction. Once agreed, any such additional instruction is deemed as a Documented Instruction under this DPA.

3.6 Treasure Data shall not disclose Personal Data to any third party except as permitted under the Agreement or as necessary to comply with the law or a valid and binding order of a governmental body. If Treasure Data is required to disclose Personal Data to a governmental body, then Treasure Data will use commercially reasonable efforts to give Customer notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Treasure Data is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Clause 3.6 varies or modifies the Standard Contractual Clauses.

3.7 Treasure Data shall ensure that persons it authorizes to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. OBLIGATIONS TO ASSIST

4.1 Upon Customer's request, Treasure Data shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under applicable Data Protection Legislation to carry out a data protection impact assessment 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 Treasure Data. Treasure Data shall provide reasonable assistance to Customer in relation to prior consultation with the competent Supervisory Authority in the performance of its tasks relating to this Clause 4.1, to the extent required under applicable Data Protection Legislation.

4.2 Treasure Data shall, to the extent legally permitted, promptly notify Customer if Treasure Data receives a request from a Data Subject to exercise the Data Subject's right granted under the applicable Data Protection Legislation ("**Data Subject Request**"). To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Treasure Data shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Treasure Data is legally permitted to do so.

4.3 Treasure Data provides assistance to Customer in relation to data security and Personal Data Breaches according to Clause 5 below.

5. DATA SECURITY AND PERSONAL DATA BREACHES

5.1 Treasure Data has implemented and will maintain appropriate technical and organizational measures ("**Security Measures**") intended to protect Personal Data Processed under the Agreement against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. Treasure Data's Security Measures applicable to the Services provided under the Service Agreement are further described at Schedule 2 to this DPA. Customer agrees that the Security Measures are appropriate for the Processing of Personal Data under the Agreement.

5.2 Customer agrees that Treasure Data may modify at any time at its discretion the Security Measures, provided that Treasure Data does not decrease the overall security of the Services during the term of the Agreement and continues to comply with Clause 5.1 above. From time to time the most up to date description of the Security Measures will be made available on Treasure Data's website (www.treasuredata.com/terms/) or communicated to Customer in writing.

5.3 In the event of a Personal Data Breach, Treasure Data shall notify Customer promptly without undue delay after becoming aware of the Personal Data Breach. The notification shall contain information that Treasure Data is reasonably able to disclose to Customer, including the following information (which may be provided in phases if it is not possible to provide the information at the same time): (a) a description of the nature of the Personal Data Breach including, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned; (b) the name and contact details of contact point where more information can be obtained; (c) a description of the likely consequences of the Personal Data Breach; and (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach. Customer shall provide notice of the Personal Data Breach to the Data Subjects and Supervisory Authority as it determines necessary.

6. SUB-PROCESSORS

6.1 Treasure Data is entitled to use Sub-processors for the purpose of providing the Services under the Agreement. Treasure Data provides information about its Sub-processors on its website (www.treasuredata.com/terms/) or otherwise in writing to Customer. Customer accepts Treasure Data's use of Sub-processors as they are listed on its website at the time of entering into the Service Agreement, those authorized by Customer pursuant to this Clause 6 and those expressly authorized by Customer under the Service Agreement (such as under a SOW). Treasure Data is entitled to reduce the number of Sub-processors without separate notice.

6.2 When adding a new Sub-processor, Treasure Data shall update the list published on its website referred to under Clause 6.1 at least 30 days before the new Sub-processor Processes Personal Data under the Agreement. Such update is deemed to be notice given to Customer about the proposed engagement of the new Sub-processor for the purpose of Clause 6.3 below, unless Customer has requested to receive any such notice via email by subscribing to email notifications about new Sub-processors by using the subscription mechanism made available by Treasure Data on its website (https://www.treasuredata.com/terms/sub-processors/). During the time Customer is subscribed, the email notification to the email address indicated by Customer when subscribing is notice given for the purpose of Clause 6.3 below.

6.3 Customer may object to Treasure Data's use of a new Sub-processor for Good Cause by notifying Treasure Data promptly in writing at legal@treasure-data.com within 14 days following notice of the new Sub-processor by Treasure Data given pursuant to Clause 6.2. If Customer objects to a new Sub-Processor pursuant to this Clause 6.3, Treasure Data may 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 new Sub-processor without unreasonably burdening Customer. If Treasure Data confirms to Customer that Treasure Data is unable to make available such change, Customer may terminate, within 14 days of receiving such confirmation, only to that part of the Services which cannot be provided without the use of the new Sub-processor by providing written notice to Treasure Data at legal@treasure-data.com. "**Good Cause**" means a justified doubt as to whether the new Sub-processor can comply with the relevant contractual requirements described in this DPA. In the event Customer terminates the Service subscription pursuant to this Clause 6.3, Treasure Data will refund Customer any prepaid fees covering the remainder of the term of Service subscription following the effective date of termination with respect to such terminated Service without any further liability to Customer in respect of such termination.

6.4 If Customer does not object to the addition of a new Sub-Processor pursuant to Clause 6.3 or if, following any such objection, Customer does not terminate the Agreement pursuant to Clause 6.3, then Customer shall be deemed to have authorized Treasure Data to use the new Sub-processor.

6.5 Treasure Data shall ensure that its Sub-processors are subject to equivalent requirements regarding confidentiality and data protection as set out in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processors. Treasure Data remains responsible towards Customer for Treasure Data's Sub-processors' acts and omissions pursuant to the Agreement

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1 Customer acknowledges that the provision of the Services may require international transfers of Personal Data, including without limitation transfers to countries not recognized under EU Data Protection Legislation as providing an adequate level of protection of personal data. Customer agrees to any such transfers, provided that Treasure Data complies with this Clause 7.

7.2 The Parties agree that where a transfer of Personal Data from Customer to Treasure Data is a Restricted Transfer:

(a) In relation to Personal Data that is protected by the EU GDPR, the EU C-to-P Transfer Clauses are deemed entered into (and incorporated into this DPA by this reference), subject to the provisions at Schedule 3 – Part 2;

(b) In relation to Personal Data that is protected by the UK GDPR, the UK Addendum is deemed entered into (and incorporated into this DPA by this reference); and

(c) In relation to Personal Data that is protected by the FDPA, the EU C-to-P Transfer Clauses, as adapted pursuant to Schedule 3, are deemed entered into (and incorporated into this DPA by this reference).

7.3 Subject to Clause 7.2, Customer agrees that Treasure Data may transfer Personal Data if required to do so by law to which Treasure Data is subject; in such a case, Treasure Data shall inform Customer of such legal requirement before transfer, unless that law prohibits Treasure Data from doing so.

7.4 If Customer is not the only Controller in respect of the Personal Data, then Customer is responsible for ensuring that its agreement with any other Controller allows for the use of all of the transfer mechanisms mentioned in this Clause 7. Customer warrants and represents that any relevant Controller has authorized Customer to agree to the transfers as described in this Clause 7.

8. AUDITS

8.1 Upon Customer's written request at reasonable intervals considering the circumstances, Treasure Data will make available to Customer such necessary information in Treasure Data's possession and control as Customer may reasonably request, with a view at demonstrating Treasure Data's compliance with the obligations of a Processor under the Data Protection Legislation in relation to Treasure Data's processing of Personal Data under this DPA.

8.2 Customer agrees to exercise any right it might have under applicable Data Protection Legislation to conduct an audit or an inspection by submitting a written request for information to Treasure Data, in which case Treasure Data may provide an audit report prepared by a respected third party which is not older than 12 months, in satisfaction of such request, so that Customer can reasonably verify Treasure Data's compliance with its obligations in relation to its Processing of Personal Data under this DPA.

8.3 Where the Standard Contractual Clauses apply between the Parties, the Parties agree that audits pursuant to the Standard Contractual Clauses may be carried out as follows: (a) in accordance with Clauses 8.1 and 8.2 above of this DPA; and/or (b) Customer may contact Treasure Data to request an audit at Treasure Data's and/or Treasure Data Subsidiaries' premises of the procedures relevant to the protection of Personal Data and shall provide Treasure Data with at least 30 days prior written notice to prepare for the onsite audit. Customer shall reimburse Treasure Data for any time expended for any such on-site audit at Treasure Data's then-current professional services rates. Before the commencement of any such on-site audit, Customer and Treasure Data shall mutually agree upon the scope, timing, and duration of the audit in addition to the audit fee for which Customer shall be responsible. Customer shall promptly notify Treasure Data at security@treasure-data.com with information regarding any non-compliance discovered during the course of an audit.

8.4 Any information or audit report shared in accordance with this Clause 8 shall be Treasure Data's Confidential Information.

9. TERM OF THE DPA AND CONSEQUENCES OF TERMINATION

9.1 This DPA shall continue in force until expiration or termination of the Service Agreement. Clauses 1, 2, 3.7, 9 and 11 shall survive termination of this DPA.

9.2 Treasure Data shall, at Customer's choice, return or delete all Personal Data in its possession within 30 days from termination or expiration of the Service Agreement ("**Post-Termination Period**"), unless otherwise required by law. Where Customer elects to have Personal Data returned to it pursuant to this Clause 9.2, Treasure Data may fulfil its obligation under this Clause 9.2 by granting Customer, at Customer's cost and expense, access to Personal Data stored in the Service during the Post-Termination Period (or any other period as it may be agreed by the Parties in writing ("**Extended Post-termination Period**")) so as to allow Customer to extract a copy of the Personal Data. Where Personal Data are not deleted by Customer, Treasure Data shall delete Personal Data in its possession within the end of the Post-Termination Period or within 30 days from the expiration of the Extended Termination Period, unless otherwise required by law.

10. CCPA COMPLIANCE

10.1 In addition to all other Clauses of this DPA, this Clause 10 applies if Customer is subject to the CCPA.

10.2 In this Clause 10, "CCPA Personal Information" means Personal Data that is "personal information" under the CCPA. All references to "Controller", "Processor" and "Data Subject" in this DPA shall be deemed to be references to, respectively, "Business", "Service Provider" and "Consumer" as defined in the CCPA. Any capitalized term used in this Clause 10 but not defined herein, shall have the meaning set forth in the CCPA.

10.3 The Parties agree that Treasure Data acts as Customer's Service Provider in respect of the Processing of CCPA Personal Information. Treasure Data shall not:

(i) retain, use or disclose CCPA Personal Information for any business or commercial purpose other than the limited and specified Business Purpose of performing the Services under the Agreement, including retaining, using, or disclosing the CCPA Personal Information for a Commercial Purpose other than the Business Purpose specified in the Agreement, or as otherwise permitted by the CCPA;

(ii) Sell or Share CCPA Personal Information;

(iii) retain, use or disclose CCPA Personal Information outside of the direct business relationship between Treasure Data and Customer, unless permitted by the CCPA; or

(iv) combine CCPA Personal Information received from, or on behalf of, Customer with other personal data it receives from, or on behalf of, another party, or personal data that Treasure Data has received from its own interactions with Data Subjects, except as permitted by the CCPA.

10.4 Treasure Data shall comply with all provisions applicable to it under the CCPA in the context of its role as a Service Provider to Customer. Treasure Data shall provide the same level of privacy protection as is required of Businesses given the nature of the CCPA Personal Information that Treasure Data receives pursuant to the Agreement. Treasure Data shall cooperate with Customer in responding to and complying with consumers' requests made pursuant to the CCPA in accordance with Clause 4 (Obligations To Assist) of this DPA. Treasure Data shall, as set forth in Clause 5 (Data Security and Personal Data Breaches) of this DPA, implement the Security Measures that the Parties agree are reasonable security procedures and practices appropriate to the nature of the CCPA Personal Information to protect such information from unauthorized or illegal access, destruction, use, modification, or disclosure.

10.5 Treasure Data will make available to Customer information sufficient to demonstrate compliance with the obligations set forth in this Clause 10 pursuant to Clause 8 (Audits) of this DPA.

10.6 Upon notice to Treasure Data, Customer may take reasonable and appropriate steps to stop and remediate the unauthorized use of CCPA Personal Information by Treasure Data. For the avoidance of doubt, reasonable and appropriate steps do not include steps that would constitute a breach of the Agreement.

10.7 Treasure Data shall enter into a written agreement with its Sub-processors and impose on each Sub-processor contractual obligations equivalent to those that Treasure Data undertakes under this Clause 10 in consideration of the services provided by the Sub-processor.

10.8 Treasure Data shall notify Customer if Treasure Data determines that it can no longer meet its obligations under the CCPA.

11. MISCELLANEOUS

11.1 Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability set out in the Service Agreement

11.2 In the event of a conflict between the provisions of this DPA and those of the Service Agreement in respect of the subject matter of this DPA, the provisions of this DPA prevail. With respect of Treasure Data's Processing of Personal Data as part of a Restricted Transfer, in the event of a conflict between the terms of the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses prevail.

11.3 No one other than a Party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

SCHEDULE 1

DETAILS OF THE PROCESSING ACTIVITIES

Subject matter of the Processing:	Provision of the Services to Customer.
Duration of the Processing:	Subject to Clause 9.2, Treasure Data Processes Personal Data for as long as is necessary for the provision of the Services.
Nature and purpose of Processing:	Treasure Data Processes Personal Data as necessary to perform the Services pursuant to the Agreement, and as it may be further specified in any technical documentation made available to Customer or further instructed by Customer pursuant to the Agreement in its use of the Services.
Types of Personal Data:	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 but are not limited to: first and last name, job title, contact information (email, phone, business and/or home address), online unique identifiers, location data, browsing history, information about personal interests. Subject to any restrictions set out under the Service Agreement, Customer may submit "special categories of personal data" (as defined under EU Data Protection Legislation) to the Services, the extent of which is determined and controlled by the Customer in its sole discretion.
Categories of Data Subjects	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, but is not limited to Personal Data relating to the following categories of data subjects: natural persons who are prospects or clients of Customer, or users of Customer's products or services or visitors of Customer's web properties.

Updated: December 28, 2022

SCHEDULE 2

SECURITY MEASURES

1. Security Measures

Treasure Data's security measures are designed to: (a) ensure the security, integrity and confidentiality of Personal Data; (b) protect against reasonably anticipated threats or hazards to the security or integrity of Personal Data; and (c) protect against unauthorized access to or use of Personal Data that could result in substantial harm or inconvenience to the person that is the subject of Personal Data.

2. General Procedures

a. Data Storage. Personal Data is protected using cryptographic means when the interfaces to it cannot be properly enumerated and protected, such as when being transmitted over a network. When the data resides in a secure location, such as on servers that are adequately controlled, it is protected using logical means, such as: database access lists and file system permissions. When using cryptography, only established and/or NIST-approved algorithms and modes of operation are used; for example, symmetric encryption is done using AES-128 or AES-256, and transport encryption is carried out using TLS and DTLS. Personal Data that is stored on Internet-facing hosts is protected by network layer access control lists, which enforce a strict ruleset on incoming traffic. Anomalous activities, such as activities which can be indicative of an emerging attack, are logged and signalled for analysis and remediation.

b. Data Transfers. Treasure Data uses HTTPS standards to protect data integrity during transfers. In addition, subject to Clause 2.a above, Treasure Data will maintain at least the following security measures: HTTP with SSL 128-bit or 256-bit encryption (HTTPS); and secure access to the Service.

c. Access and Use Monitoring. Treasure Data will monitor Treasure Data's user access to and use of the Service for security, performance evaluation, and system utilization purposes.

3. Security reviews of the operations environment

The operations environment is repeatedly reviewed in design and actual execution. The latter is accomplished using penetration tests that are carried out by Treasure Data and external service providers. A summary of those reviews can be shared with Customer provided that the content may be redacted as necessary to ensure the confidentiality and security of the environment for other Treasure Data customers.

Treasure Data has experience in supporting external audits by third parties on behalf of customers. In such situations, some of the internal security review material can be shared with the external auditor to facilitate a more thorough review for lesser costs.

4. Network security

Network security is a wide security domain that is addressed at multiple levels, some of which are: (a) reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources; (b) strong network layer access controls; (c) patch management and vulnerability management; (d) secure authentication supporting multiple robustness levels, according to the privilege of the account to which the user authenticates; (e) proper logging and signalling of both successful and failed attempts; (f) secure administrative remote access to the service network; and (f) proper utilization of key management mechanisms utilizing hardware and/or software.

5. Backup and Business Continuity

Treasure Data maintains a business continuity program, including a recovery plan, designed to ensure Treasure Data can continue to function and provide Service to Customer through an operational interruption. The program provides a framework and methodology,

including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions. If Treasure Data experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly. Treasure Data continuously enhances the security and availability of its multi–tenant enterprise class cloud infrastructure.

6. Key Management

Encryption keys are used all around the hosted software application that are used to provide the Service. They are used for secure storage, secure transport, token generation, and authentication. The hosted software application used to provide the Service does not utilize a single centralized key-store for both architecture and security reasons. Different keys are stored by different means in accordance with their availability and security requirements.

SCHEDULE 3

SCHEDULE 3 – PART 1
APPENDIX TO THE EU C-TO-P TRANSFER CLAUSES

The Appendix to the EU C-to-P Transfer Clauses is completed as follows:

ANNEX I

A. LIST OF THE PARTIES

Data exporter:

Name: Customer (as identified in the Service Agreement)

Address: as specified in the Service Agreement

Contact person's name, position and contact details: as identified in the Service Agreement

Activities relevant to the data transferred under these Clauses: Performance of the Services pursuant to the Service Agreement

Role (controller/processor)*:* Controller

Data importer:

Name: Treasure Data, Inc.

Address: as specified in the Service Agreement

Contact details: Treasure Data Privacy and Security Team, privacy@treasure-data.com

Activities relevant to the data transferred under these Clauses: Performance of the Services pursuant to the Service Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As detailed in Schedule 1

Categories of personal data transferred

As detailed in Schedule 1

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

As detailed in Schedule 1

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

On a continuous basis depending on the use of the Services by Customer.

Nature of the processing

As detailed in Schedule 1

Purpose(s) of the data transfer and further processing

The purpose is the provision of the Services by Treasure Data under the Service Agreement.

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

For the duration of the Agreement, subject to Clause 9.2 of the DPA or different instructions from Customer given pursuant to the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As detailed on Treasure Data's website: https://www.treasuredata.com/terms/sub-processors/ or otherwise expressly specified under the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

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

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

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

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

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural person.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

As detailed in Schedule 2 to this DPA

ANNEX III: LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

As detailed in Clause 6 of this DPA

SCHEDULE 3 – PART 2:
OPERATIVE AND ADDITIONAL PROVISIONS FOR THE EU C-TO-P TRANSFER CLAUSES

Unless otherwise specified, any reference to a "Clause" under this Schedule 3 – Part 2 is a reference to the relevant Clause in the EU Transfer Clauses.

1. **Liability.** Any claims brought by a Party against the other Party under the EU Transfer Clauses shall be subject to the Agreement, including without limitation the terms and conditions governing limitations of liability. Clause 11.1 of this DPA and the limitations of liability provisions of the Service Agreement constitute additional clauses pursuant to Clause 2.

2. **Docking clause**. The optional Clause 7 does not apply.

3. **Instructions**. The Documented Instructions under Clause 3 of this DPA are deemed to be the instructions by Customer for the purpose of Clause 8.1. For the purposes of Clause 8.1(a) the instructions by Customer to Process Personal Data include onward transfers to third parties located outside the EEA, UK or Switzerland for the purpose of the performance of the Services.

4. **Sub-processors.** Option 2 (General Written Authorisation) under Clause 9 (a) applies. Customer acknowledges and expressly agrees that pursuant to Clause 9(a), information about Treasure Data's Sub-processors is given as described in Clause 6 of this DPA and that Treasure Data may engage new Sub-processors as described in Clause 6 of this DPA. Where Treasure Data enters into the EU P-to-P Transfer Clauses with a Sub-processor, Customer hereby grants Treasure Data authority to provide a general authorisation on Customer's behalf for the engagement of sub-processors by the Sub-processor, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

5. **Certification of deletion**. Parties agree that the certification of deletion of Personal Data that is described in Clauses 8.5 and 16(d) shall be provided by Treasure Data to Customer upon Customer's written request.

6. **Redress.** In Clause 11, the optional language does not apply.

7. **Notifications to Data Subjects**. For the purposes of Clause 15(1)(a), Treasure Data shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

8. **Governing law**. For the purpose of Clause 17, the governing law shall be that governing the Service Agreement, as designated thereunder. If the Service Agreement is not governed by an EU Member State law that allows for third-party beneficiary rights, the EU C-to-P Transfer Clauses shall be governed by the laws of Ireland.

9. **Choice of forum and jurisdiction**. For the purpose of Clause 18(b), the competent courts shall be those identified in the Service Agreement. If the Service Agreement does not designate the courts of a EU Member State as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with the EU C-to-P Transfer Clauses, the Parties agree that the competent courts under Clause 18(b) shall be those of Ireland.

SCHEDULE 3 – PART 3:
RELEVANT TRANSFERS SUBJECT TO THE FDPA

In respect of any Restricted Transfer of Personal Data subject to the FDPA, the EU C-to-P Transfer Clauses are adapted as follows. The provisions below are additional to those set out in Schedule 3 – Part 1 and Part 2 above and prevail in case of any conflict to the extent the Relevant Transfer is governed under the FDPA:

1. the competent supervisory authority in Annex I.C of the EU C-to-P Transfer Clauses is the Swiss supervisory authority. If the Restricted Transfer is subject to both the FDPA and the GDPR, then a parallel supervision takes place: the Swiss supervisory authority, insofar as the Restricted Transfer is governed by the FDPA; the competent EU authority insofar as the Restricted Transfer is governed by the GDPR (the criteria of Clause 13(a) for the selection of the competent authority must be observed);
2. the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU C-to-P Transfer Clauses;
3. general references to the GDPR in the EU C-to-P Transfer Clauses are to be understood as references to the FDPA;
4. references to specific articles of the GDPR are replaced with the equivalent article or section of the FDPA, as far as the Relevant Transfer is subject to the FDPA;
5. the articles of the EU C-to-P Transfer Clauses also protect the data of identified or identifiable legal entities that is Collected Data for so long as such data is afforded the same protection of Personal Data under the FDPA;
6. references to 'EU', 'Union' and 'Member State' are replaced with 'Switzerland';
7. Clause 13(a) and Part C of Annex 2 is not used, and the 'competent supervisory authority' is the Swiss Federal Data Protection Information Commissioner ("FDPIC");
8. references to the 'competent supervisory authority' and 'competent courts' are replaced with the FDPIC and 'competent Swiss court;

9. in Clause 17, the EU C-to-P Transfer Clauses are governed by the laws of Switzerland; and
10. in Clause 18(b), disputes will be resolved before the competent Swiss court.

SCHEDULE 3 – PART 4
RELEVANT TRANSFERS SUBJECT TO THE UK GDPR

To the extent any Restricted Transfer of Personal Data is subject to the UK GDPR, the UK Addendum as integrated under this Schedule 3 – Part 4 applies.

In the UK Addendum:
Tables 1, 2 and 3 are completed as per details provided in Schedule 3 – Part 1 of this DPA
Table 4: Neither Party may end the UK Addendum as set out in Section 19 of such UK Addendum.