CAMELO DATA PROCESSING ADDENDUM

Last updated on 14 September 2024.

This Data Processing Addendum ("**DPA**") supplements, and forms part of, the User Terms or the Subscription Agreement (the "**Agreement**") between the applicable Camelo contracting entity ("**Camelo**") and the entity or person(s) identified as Customer in the relevant account or Agreement (as applicable) ("**Customer**").

This DPA applies where and to the extent that Camelo is acting as a processor and/or controller of personal data on behalf of Customer under the Agreement. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of such conflict. In the event of any conflict between the SCCs (defined in Section 1 below) and the Agreement (including this DPA), the SCCs shall prevail to the extent of such conflict.

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions. In this DPA, the following terms shall have the following meanings:

"**Applicable Data Protection Laws**" means the US Data Protection Laws and the European Data Protection Laws that are applicable to the processing of personal data under this DPA.

"**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given to them in the European Data Protection Laws.

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

"**EEA/UK Adequate Countries**" means: (a) in respect of personal data which is subject to the EU GDPR, the EEA and any other territory which the European Commission has determined ensures an adequate level of protection of personal data pursuant to Article 45 of the EU GDPR; and (b) in respect of personal data which is subject to the UK GDPR, the United Kingdom and any other territory which the UK Secretary of State has determined, by regulations, ensures an adequate level of protection of personal data pursuant to Article 45 of the UK GDPR and Section 17A of the UK Data Protection Act 2018.

"**European Data Protection Laws**" means: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (b) the GDPR as incorporated into United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (c) EU Directive 2002/58/EC on Privacy and Electronic Communications; and (d) any EU Member State or United Kingdom law made under or pursuant to items (a) – (c); in each case as updated, amended, replaced or superseded from time to time.

"**Restricted Transfer**" means a transfer of personal data that is subject to European Data Protection Laws outside the EEA/UK Adequate Countries.

"**SCCs**" means: (a) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**"); and (b) where the UK GDPR applies, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR (the "**UK SCCs**"); in each case as updated, amended, replaced or superseded from time to time.

"**Security Incident**" means any accidental or unlawful destruction, loss or alteration of personal data, or any unauthorised disclosure of or access to personal data.

"**Sub-processor**" means any processor engaged by Camelo to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement where such entity processes Data (as defined in Section 2.1(a) below). Sub-processors may include Camelo's affiliates or other third parties.

"**US Data Protection Laws**" means all data protection or privacy laws and regulations applicable to the personal data in question in force within the United States, including the California Consumer Privacy Act (as amended from time to time) (the "**CCPA**"), and any rules or regulations implementing the foregoing.

1.2 **Interpretation.** Capitalised terms used but not defined in this DPA shall have the meanings given to them in the Agreement.

2. PROCESSING OF PERSONAL DATA

2.1 Relationship of the parties.

(a) **Camelo as a processor**. The parties acknowledge that, except as set out in Section 2.1(b), Customer shall act as a controller and Camelo shall act as a processor in respect of its processing of the personal data of Authorised Users (the "**Data**") disclosed to Camelo for the purpose of Camelo providing the Services.

(b) **Camelo as a controller**. The parties acknowledge that Customer acts as a controller and Camelo may also act as a controller in respect of its processing of the Data to: (i) comply with its own obligations under applicable law and regulations and to establish, exercise or defend legal claims; (ii) contact Authorised Users in relation to the Services and/or any Third Party Products and Services; (iii) provide any services directly to Authorised Users, other than the Services provided to Customer; (iv) facilitate the provision of Third Party Products and Services to Authorised Users; (v) conduct research and development and improve the Services in a way that is not specific to Customer; (vi) communicate directly with Authorised Users, other than for the purpose of providing the Services to Customer; (vii) protect the safety and security of the Services in a way that is not specific to Customer, including detecting and responding to Security Incidents or malicious and unlawful activity; (viii) generate de-identified statistical data to uncover collective insights about the use of the Services (and not to specifically analyse personal characteristics); and/or (ix) process such Data in any other context which requires Camelo to determine the purposes and means of such processing.

2.2 **Prohibited Data.** Customer will not disclose (and will not permit any Authorised User to disclose) any special categories of personal data to Camelo for processing.

2.3 **Purpose Limitation.** Camelo shall process the Data as necessary to perform its obligations under the Agreement and strictly in accordance with the documented lawful instructions of Customer (including the terms of the Agreement), or as otherwise agreed in writing by the parties (the "**Permitted Purpose**"). Camelo shall not use, disclose or otherwise process the Data for any other purpose other than the Permitted Purpose, except where otherwise required by any law applicable to Camelo, and shall not "sell" the Data within the meaning of the CCPA or otherwise.

2.4 **Security.** Camelo shall implement appropriate technical and organisational measures to protect the Data against a Security Incident and to preserve the security and confidentiality of the Data, in accordance with Camelo's security standards (Security Measures). Customer acknowledges that the Security Measures are subject to technical progress and development and that Camelo may update or modify the Security Measures from time to time.

2.5 **Security Incidents.** Upon becoming aware of a Security Incident, Camelo shall notify Customer without undue delay by written notice with all relevant details reasonably available of the Security Incident to allow Customer to fulfil its data breach reporting obligations under Applicable Data Protection Laws. Customer shall take further steps to contain, investigate and mitigate the effects of the Security Incident. Camelo’s notification of or response to a Security Incident in accordance with this Section 2.5 will not be construed as an acknowledgement by Camelo of any fault or liability with respect to the Security Incident.

2.6 **Confidentiality.** Camelo shall take reasonable steps to ensure that it has appropriate policies and procedures in place in relation to any person that it authorises to process the Data (including Camelo’s employees, agents and Sub-processors) and to ensure that such persons are subject to a duty of confidentiality.

2.7 **Deletion or return of the Data.** Upon written request from Customer, Camelo shall anonymise, delete or return to Customer all Data in its possession or control subject to any requirement on Camelo to retain some or all of the Data to comply with applicable laws, in which event Camelo shall isolate and protect the Data from further processing except to the extent required by such law until deletion is possible. Customer acknowledges that there may also be circumstances in which one or more of its Authorised Users are Authorised Users of one or more other customers and in such circumstances, Camelo will continue to process the applicable Data related to such Authorised User(s) until a written request from such Authorised User(s) is received by Camelo in accordance with this Section 2.7.

2.8 **Cooperation and data subjects’ rights.** Camelo shall provide reasonable assistance to Customer (at Customer’s expense) to enable Customer to respond to: (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Laws (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party, in each case in respect of Data that Camelo processes on Customer’s behalf. In the event that any request, correspondence, enquiry or complaint is made directly to Camelo, Camelo shall promptly notify Customer and provide it with a copy of the request, unless legally prohibited from doing so.

2.9 **Data Protection Impact Assessment.** Camelo shall provide reasonable assistance to Customer (at Customer's expense) with undertaking an assessment of the impact of processing the Data, and with any consultations with a data protection authority, if and to the extent an assessment or consultation is required to be carried out under the Applicable Data Protection Laws**.**

2.10 **Audits.** Upon written request from Customer, Camelo shall: (a) supply a copy of its DPA; and (b) respond to reasonable written audit questions submitted to it by Customer (such responses will be in the manner and form that Camelo generally makes such responses available to its customers), provided that Customer shall not exercise this right more than once per year. Customer agrees that Customer shall exercise its rights by instructing Camelo to comply with the audit measures described in this Section 2.10. The parties agree that they shall, prior to any audit (at Customer's expense), agree on the scope of the audit and any reasonable limitations or conditions applicable to such audit. All such audits shall be conducted:

(a) on reasonable written notice to Camelo;

(b) only during Camelo's normal business hours; and

(c) in a manner that does not disrupt Camelo's business;

2.11 **Sub-processors.** Customer agrees that Camelo may engage Sub-processors to process the Data for the Permitted Purpose. The Sub-processors currently engaged by Camelo and authorised by Customer are listed at the below ANNEX 3. Camelo shall ensure that: (a) there is a written agreement in place with each Sub-processor that imposes terms and conditions that require the relevant Sub-processor to protect the Data to the standard required by the Applicable Data Protection Laws; and (b) it remains responsible to Customer for the performance of such Sub-processors data protection obligations under such terms and conditions. Camelo shall notify Customer if it adds or replaces any new Sub-processors at least 20 days before the proposed addition or replacement, in order to allow Customer to raise any reasonable objections on grounds of data protection.

2.12 **Restricted Transfers.** The parties agree that when the transfer of Data from Customer (as “data exporter”) to Camelo (as “data importer”) is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards be put in place, it shall be subject to the appropriate SCCs, which shall be deemed incorporated into and form part of this DPA, as follows:

(a) in relation to transfers of Data protected by the EU GDPR and processed in accordance with Section 2.1(a), the EU SCCs shall apply and be completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9(a), Option 2 will apply, and the time period for prior notice of Sub-processor changes is as set out in Section 2.11 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;

(vi) in Clause 18(b), disputes will be resolved before the courts of Ireland; and

(vii) the Annexes of the EU SCCs shall be populated with the information set out in the corresponding Annexes to this DPA;

(b) in relation to transfers of Data protected by the EU GDPR and processed in accordance with Section 2.1(b), the EU SCCs shall apply and be completed as follows:

(i) Module One will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;

(v) in Clause 18(b), disputes will be resolved before the courts of Ireland; and

(vi) the Annexes of the EU SCCs shall be populated with the information set out in the corresponding Annexes to this DPA; and

(c) in relation to transfers of Data protected by the UK GDPR, the UK SCCs will apply and the relevant Annexes or Appendices of the UK SCCs will be populated with the relevant information set out in the Annexes to this DPA, noting the UK SCCs will be governed by the laws of Ireland and all disputes will be resolved before the courts of Ireland.

2.13 **General Customer obligations.** Without limiting Customer’s other obligations under the Agreement, Customer shall: (a) comply at all times with the Applicable Data Protection Laws in its processing of Data, including (but not limited to) when Customer discloses Data to

Camelo under the Agreement, and provide Camelo with such cooperation, assistance and information as Camelo may reasonably request to comply with its obligations under the Applicable Data Protection Laws; (b) ensure that any instructions it issues to Camelo comply with the Applicable Data Protection Laws; (c) ensure that it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Laws to process personal data (including but not limited to any special categories of data) and to enable Camelo to provide the Services pursuant to the Agreement (including this DPA); (d) ensure that any Data provided to Camelo is limited to only what is necessary in order for Camelo to provide the Services and such Data is accurate and up- to-date to the best of Customer's knowledge at the time that it is provided to Camelo; (e) use all reasonable endeavours to promptly notify Camelo upon becoming aware that Data has become inaccurate or out of date; and (f) not do or permit to be done anything within its knowledge or control which may cause or otherwise result in Camelo being in breach of the Applicable Data Protection Laws.

2.14 **Exclusions and limitations of liability.** Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party’s affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

ANNEX 1

DESCRIPTION OF THE PROCESSING ACTIVITIES / TRANSFER

ANNEX 1A: LIST OF PARTIES

Data exporter

Name: Customer (as identified in the Agreement).

Address: Customer's address (as identified in the Agreement).

Contact Person's name, position and contact details: Customer Contact Name and corresponding details (as identified in the Agreement).

Activities relevant to the transfer: Refer to Annex 1B below.

Role: Controller.

Data importer

Name: The Camelo contracting entity (as identified in the Agreement).

Address: The Camelo contracting entity's address (as identified in the Agreement).

Contact Person's name, position and contact details: Brian Le, CEO, brian@camelohq.com

Activities relevant to the transfer: Refer to Annex 1B below.

Role: Processor and/or controller.

ANNEX 1B: DESCRIPTION OF PROCESSING / TRANSFER

Categories of data subjects

- Authorised Users
- Customers

Categories of personal data

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and photo;
- Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, and driving licence details;
- Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, and professional expertise;
- Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, shift and attendance records, health and safety records, performance appraisals, training records, and security records;
- Financial details, including information relating to the financial affairs of the data subject, including bank account details, income, and payroll information;

- Device data, including connection type and settings, operating system, browser type, IP address, time zone settings, the time spent on webpages, unique device identifiers, cookies, online tracking data, geolocation data and other diagnostic data; and
- Content created by Customer or data subjects and submitted to a Camelo technology platform.

Special categories of personal data

- Biometric information.

Other special categories of personal data may be processed by Camelo, from time to time, in circumstances where Customer or its Authorised Users choose to disclose special categories of personal data using the Services. Customer is responsible for ensuring that suitable safeguards are in place prior to disclosing, or prior to permitting its Authorised Users to disclose, any other special categories of personal data using the Services.

Frequency of the transfer

Continuous.

Nature and purpose of the processing

The nature and purpose of processing personal data is to enable the functionality of the Camelo platform as set out in the Agreement and related documentation.

Duration of the processing

Processing of the personal data will continue for the duration of the Agreement.

ANNEX 1C: COMPETENT SUPERVISORY AUTHORITY

Processing of personal data to which the EU GDPR applies

The competent supervisory authority shall be the supervisory authority:

- applicable to the data exporter in its country of establishment in the EEA; or
- where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed; or
- where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

Processing of personal to which the UK GDPR applies

The Information Commissioner's Office.

ANNEX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Camelo implements a variety of technical and organisational security measures.

Part 1

Security

Introduction

Camelo employs a combination of policies, procedures, guidelines, and technical and physical controls to protect the personal data it processes from accidental loss and unauthorised access, disclosure, or destruction.

Governance and Policies

Camelo assigns personnel with responsibility for the determination, review and implementation of security polices and measures.

Camelo reviews its security measures and policies on a regular basis to ensure they continue to be appropriate for the data being protected.

Camelo establishes and follows secure configurations for systems and software and ensures that security measures are considered during product development and deployment.

Breach response

Camelo's disaster recovery and business continuity plans are tested and updated at least once quarterly.

Camelo performs a monthly full restore from a recent point-in-time backup into a non-production environment where functional validation is performed.

Access controls

Camelo allows Customers to access uploaded by them or stored on their behalf through Camelo's GraphQL API.

Camelo limits access to personal data by implementing appropriate access controls, including:

- limiting internal administrative access privileges and use of administrative accounts following the principle of least privilege, and ensuring that access is appropriate with regard to the authentication method and the user's business function;
- limiting access to production environments through VPN and AWS identity access

management;

- use of password management best practices for internal password expiry and rotation;
- requiring personnel to use multi-factor authentication to gain access to IT systems;
-
- only permitting user access to personal data which the user needs to access for his/her/their job role or the purpose they are given access to Camelo's IT systems for (i.e. Camelo implements measures to ensure least privilege access to IT systems);
- zencouraging users to use strong passwords, such as passwords with over eight characters, combination of upper and lower case letters, numbers and special characters;
- engineering resources use passwords that are encrypted and scrubbed ahead of movement within systems;
- systems administrators and customer care staff are required to use multi-factor authentication tied to Camelo-managed credentials using standard methods such as gpg signed keys, and Google Authentication;
- automatic timeout and locking of terminals used by Camelo personnel if left idle;
-
- access to IT system is blocked after multiple failed attempts to enter correct authentication and/or authorisation details;
- monitoring and logging access to IT systems;
-
- monitoring and logging amendments to data or files on IT systems.

Availability and Back-up personal data

Camelo has a documented disaster recovery plan that ensures that key systems and data can be restored in a timely manner in the event of a physical or technical incident.

Camelo performs point-in-time back-end storage snapshots at five-minute intervals. Retention process is managed with alerts for successful backups.

Customer-facing software is hosted in AWS infrastructure with AWS KMS-managed encryption at rest with availability zone failover and cross-region replication within the USA.

Segmentation of personal data

Camelo:

- separates and limits access between network components and, where appropriate, implements measures to provide for separate processing (storage, amendment, deletion, transmission) of personal data collected and used for different purposes;
- does not use live data for testing its systems;
- data segregation by UUID.

Disposal of IT equipment

Camelo:

- has in place processes to securely remove all personal data before disposing of IT systems;
- uses appropriate technology to purge equipment of data and/or destroy hard disks.

Encryption

Camelo uses encryption technology where appropriate to protect personal data held electronically, including:

- AWS KMS-managed (AES256) encryption at rest;

Transmission or transport of personal data

Appropriate controls are implemented by Camelo to secure personal data during transmission or transit, including:

- use of VPNs;
- encryption in transit using TLS 1.2 over HTTPS using a strong cipher suite;
- ensuring physical security for personal data when transported on portable electronic devices or in paper form.

Device hardening

Camelo removes unused software and services from devices used to process personal data.

Camelo ensures that default passwords that are provided by hardware and software producers are not used.

Asset and Software management

Camelo stores all API keys securely, including as follows:

- Camelo stores API keys directly in its environment variables;
- API keys are provided to customers for access to their data and terminated upon termination of the agreement.

Staff training and awareness

Camelo's agreements with staff and contractors and employee handbooks set out its personnel's responsibilities in relation to information security.

Camelo carries out:

- regular staff training on data security and privacy issues relevant to their job role and ensures that new starters receive appropriate training before they start their role (as part of the on boarding procedures);
- appropriate screening and background checks on individuals that have access to sensitive personal data.

Camelo ensures that information security responsibilities that are applicable immediately before termination or change of employment and those which apply after termination / change of employment are communicated and implemented.

Staff are subject to disciplinary measures for breaches of Camelo’s policies and procedures relating to data privacy and security.

Selection of service providers and commission of services

Camelo assesses service providers’ ability to meet their security requirements before engaging them.

Part 2

Assistance with Data Subject Rights Requests

Camelo has implemented appropriate policies and measures to identify and address data subject rights requests, including:

- the data processed on behalf of the Customer is stored separately from data processed by Camelo;
- Camelo maintains accurate records to enable it to identify quickly all personal data processed on behalf of Camelo;

ANNEX 3

LIST OF SUB-PROCESSORS

Subprocessor	Subprocessor Function	Technical and organizational measures to assist the Customer
Amazon Web Services, Inc. (AWS)	Cloud service provider used to host, process, and store data submitted to the Service.	As described at: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Crisp IM SAS.	Customer service platform, including online helpdesk ticketing service and customer support live chat.	As described at: https://crisp.chat/en/privacy/
Posthog, Inc.	Product features and data analytics platform provider	As described at: https://posthog.com/dpa
Stripe, Inc.	On-line payment processing	As described at: https://stripe.com/dpa/legal
Google, Inc.	Workplace (*f/k/a* G-suite) Cloud-based collaboration tools and productivity applications, including hosted email and Maps for geolocation data found in the attendance feature of the Service	As described at: https://cloud.google.com/terms/data-processing - terms
Twilio Inc.	Optional cloud communication platform to send messages and images from Camelo customers to their users (and, if enabled, between users of the same account) in real time (web and mobile)	As described at: https://www.twilio.com/legal/data-protection-addendum