SCHEDULE 4 TO THE GTC

Data Processing Agreement

Version 2026-10 Published 18 October 2026, updated 19 October 2026 Wecheer SA, Lausanne

This Data Processing Agreement (**DPA**) forms part of the Agreement between Wecheer SA (CHE-304.343.601), avenue Victor-Ruffy 5, 1012 Lausanne, Switzerland (**Provider**) and the client identified in the Order Form (**Client**). It is accepted by the signature or online acceptance of the Order Form; no separate signature is required. A countersigned copy is available on request at privacy@wecheer.io.

1. Definitions and Scope

1.1 Purpose. This DPA governs the processing of personal data in connection with the Services. In case of conflict between the Agreement and this DPA with respect to the processing of personal data, this DPA prevails.

1.2 Definitions. Capitalized terms not defined here have the meaning given in the Agreement. **Applicable Data Protection Laws** means all laws applicable to the processing of personal data under the Agreement, including the Swiss Federal Act on Data Protection (FADP), the EU/EEA General Data Protection Regulation 2016/679 (GDPR) and the UK GDPR, as applicable. **Campaign Participant Data** means personal data relating to Campaign Participants taking part in a Program. **Program Administration Data** means personal data processed for Program administration, eligibility validation, reward accrual and redemption, and communications performed on Client's behalf. **Platform Account Data** means personal data processed by Provider for Platform-level purposes: registration, login and account management of Campaign Participants, safety, security, service communications and aggregated analytics. **SCCs** means the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021. The terms controller, processor, data subject, personal data, processing and personal data breach have the meanings given in Applicable Data Protection Laws.

1.3 Details of Processing. The subject matter, duration, nature and purposes of the processing, and the categories of personal data and data subjects, are set out in Annex A.

1.4 Consumer-Facing Terms. This DPA governs the business-to-business relationship between Provider and Client only. The relationship between the Platform and Campaign Participants is governed by the End-User Documentation, which each Campaign Participant accepts at account creation and Program opt-in. Access by Client's own back-office users is governed by the Agreement.

2. Roles of the Parties

2.1 Three Processing Contexts. Consistent with the information given to data subjects in the End-User Documentation, personal data is processed in three contexts: (i) Provider acts as independent controller of Platform Account Data; (ii) Provider acts as processor of Program Administration Data, on Client's documented instructions, Client acting as controller; and (iii) where the Parties jointly determine the purposes and means of processing Campaign Participant Data, namely for Program mechanics recorded as co-designed in the Order Form or in the Program brief agreed between them, they act as joint controllers, with the allocation of responsibilities set out in Annex D.

2.2 No Sale, No Third-Party Advertising. Provider does not sell Campaign Participant Data, does not share it with any advertiser other than Client (for the Programs the data subject opted into), and does not use it for third-party advertising.

2.3 Instructions. The Agreement, this DPA and the Order Form are Client's complete and documented instructions for the processing of Program Administration Data. Additional or modified instructions require the written agreement of both Parties. Provider informs Client without undue delay if, in its opinion, an instruction infringes Applicable Data Protection Laws.

2.4 Fraud Prevention. Provider processes fraud signals at Platform level, as controller, as described in Section 7.3 of the GTC. No Client Materials, Program content or Campaign Participant identity is disclosed to any other client through this processing.

3. Obligations of the Parties

3.1 Provider as Processor. When processing Program Administration Data as processor, Provider: (a) processes it only on Client's documented instructions, including with regard to international transfers, unless required otherwise by law (in which case Provider informs Client beforehand, unless prohibited by law); (b) ensures that persons authorized to process it are bound by confidentiality obligations; (c) implements the measures of Annex B; (d) respects the conditions of Section 5 for engaging sub-processors; (e) assists Client, taking into account the nature of the processing, in responding to data subject requests; (f) assists Client with security, breach notification, data protection impact assessments and prior consultations, taking into account the nature of the processing and the information available to Provider; (g) deletes or returns the data on termination in accordance with Section 9; and (h) makes available the information reasonably necessary to demonstrate compliance in accordance with Section 10.

3.2 Client as Controller. When acting as controller of Program Administration Data, Client: (a) has and maintains a valid legal basis for the processing it instructs; (b) ensures that its instructions comply with Applicable Data Protection Laws; (c) is responsible for the accuracy and lawfulness of its Program terms and the content it provides; (d) is responsible, as independent controller, for any personal data it receives into its own systems, including through data routers, including its security, its further use for marketing and the handling of data subject requests relating to it; and (e) does not instruct the processing of special categories of personal data or of data of minors.

3.3 Provider as Controller. When acting as controller of Platform Account Data, Provider complies with Applicable Data Protection Laws and processes that data in accordance with the End-User Documentation and Section 2.2.

4. Security

4.1 Measures. Provider implements and maintains the technical and organizational measures set out in Annex B, which may be updated provided the level of protection is not materially reduced.

4.2 Personnel. Provider ensures that its personnel and contractors with access to personal data are bound by confidentiality obligations and receive appropriate information security training.

5. Sub-processors

5.1 General Authorization. Client authorizes Provider to engage the sub-processors listed in Annex C. Provider imposes on each sub-processor, by written agreement, data protection obligations at least as protective as those of this DPA, and remains fully liable to Client for each sub-processor's performance.

5.2 Changes. Provider notifies Client by email, at least thirty (30) days before engaging a new sub-processor or replacing an existing one, and publishes an updated Annex C. Client may object on reasonable data protection grounds within that period. The Parties then cooperate in good faith to find a solution, which may include Provider not using the new sub-processor for Client's data or, where no solution is found, termination of the affected Services without penalty, Fees for the period already elapsed remaining due.

6. International Transfers

6.1 Hosting. The Platform is hosted on Amazon Web Services and personal data is stored in Singapore. Personal data may also be processed by the sub-processors, and in the locations, listed in Annex C. Content delivered to Campaign Participants through the content delivery network, including images they submit, may be cached temporarily at edge locations close to them.

6.2 Transfer Mechanism. Where personal data originating from the EEA, the UK or Switzerland is transferred to a country without an adequacy decision, the Parties rely on the SCCs (module two, controller to processor, and module one, controller to controller, as applicable), which are incorporated into this DPA by reference and completed with the information in Annexes A, B and C. For transfers subject to the UK GDPR, the UK International Data Transfer Addendum applies. For personal data subject to the FADP, the SCCs apply with these changes: references to the GDPR are read as references to the FADP; the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC); references to EU Member States are replaced by Switzerland; and the SCCs are governed by Swiss law, with disputes before the courts of Switzerland. Where the laws of another jurisdiction require a transfer mechanism, the Parties put it in place before the relevant Program goes live.

7. Data Subject Rights

7.1 Self-Service. The consumer-facing Wecheer application provides Campaign Participants with self-service tools to access and update their profile, manage their communication preferences, leave a Program and delete their account. After a deletion request, the account enters a 30-day dormant period during which the data subject can reactivate it; after 30 days the account is permanently deactivated and the personal data deleted or anonymized, unless retention is required by law.

7.2 Assistance. Provider notifies Client without undue delay of any data subject request relating to Program Administration Data that it receives directly, and does not respond to it other than to direct the data subject to Client or to the self-service tools, unless Client instructs otherwise or the law requires it. Provider provides reasonable assistance to Client in responding to such requests.

8. Personal Data Breach

8.1 Notification. Provider notifies Client without undue delay, and in any event within 48 hours of becoming aware of it, of a personal data breach affecting Client's Program Administration Data or Campaign Participant Data. The notification includes, to the extent available: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information may be provided in phases.

8.2 Cooperation. Provider cooperates with Client and takes reasonable steps to mitigate the effects of the breach. Provider's notification of, or response to, a breach is not an acknowledgment of fault or liability.

9. Retention, Deletion and Return

9.1 During the Term. Provider retains personal data for as long as the relevant data subject's account is active and as necessary to provide the Services. Client may instruct the deletion of Program Administration Data relating to its Programs at any time, and Provider complies within a reasonable time, except where retention is required by law (for example for fraud prevention or tax). Receipt and product images submitted for validation are retained for the duration of the relevant Program and for no longer than 180 days after submission, then deleted; the extracted data and validation results are retained in accordance with this Section 9. Before deletion, Provider may irreversibly de-identify these images by removing any link to the Campaign Participant's account, deleting their metadata and masking any personal details they show, and may retain the de-identified images for up to three (3) years from submission, including after termination of the Agreement, solely to improve and test the Platform's validation, fraud-prevention and AI functions. De-identified images are not shared with other clients or with any third party other than Provider's Sub-processors, and Section 9.2 does not apply to them. Campaign Participants are informed of this use in the End-User Documentation and may object to it.

9.2 On Termination. On termination or expiry of the Agreement, Provider, at Client's choice, returns a final extract of the Program Administration Data and/or deletes or anonymizes it within 60 days, unless retention is required by law. Copies in encrypted backups are not restored except for disaster recovery and expire automatically at the end of the backup cycle, at the latest 30 days after deletion of the production data.

10. Audit

10.1 Information. On reasonable written request, Provider makes available the information reasonably necessary to demonstrate compliance with this DPA, including answers to security questionnaires, summaries of penetration test results and copies of relevant policies.

10.2 Audit Rights. Where that information is not reasonably sufficient, Client may audit Provider's processing under this DPA, itself or through an independent auditor bound by confidentiality who is not a competitor of Provider, subject to: no more than one audit per 12-month period, except after a personal data breach or where a supervisory authority requires it; at least 30 days' prior written notice; business hours; no disruption of Provider's operations; no access to other clients' data; and each Party bearing its own costs.

11. Miscellaneous

11.1 Liability. Each Party's liability under this DPA is subject to the limitations and exclusions of the Agreement, except where Applicable Data Protection Laws do not permit them.

11.2 Term. This DPA applies for as long as Provider processes personal data in connection with the Agreement.

11.3 Precedence and Governing Law. In case of conflict, the following order applies: (1) the SCCs, where applicable; (2) this DPA; (3) the rest of the Agreement. This DPA is governed by the law of the Agreement, except where Applicable Data Protection Laws require otherwise.

11.4 Contact. Provider's privacy contact: privacy@wecheer.io.

Annex A. Details of Processing

ITEM	DETAILS
Subject matter	Provision of the Wecheer platform and related Services under the Agreement.
Duration	The Term of the Agreement, plus the deletion or return period of Section 9.

ITEM	DETAILS
Nature and purposes	Hosting and operation of Programs; opt-in and consent capture; validation of purchase actions (receipt reading, product image recognition, QR codes, unique codes and links); reward accrual and redemption; Program communications (WhatsApp, SMS, email, push) on Client's behalf; fraud prevention; reporting and dashboards; data export to Client's systems through data routers; irreversible de-identification of receipt and product images to improve and test the Platform's validation, fraud-prevention and AI functions (Section 9.1).
Data subjects	Consumers taking part in Client's Programs (18 and over only); Client's trade and staff users, where applicable.
Personal data	Account and profile data (name, email, phone, country, language, date of birth, profile photo); Program and transaction data (joins and leaves, receipt images and extracted data, product photos, QR scans, unique codes and links, geolocation where relevant, redemption history, reward delivery and redemption verification data, balances, fraud signals); device and usage data (IP address, device identifiers, app activity); communications and preferences (opt-ins, marketing preferences, contact history); age verification images or identity document data, only where age verification is ordered.
Special categories	None intended. The Platform is not designed for special categories of data, and Client does not instruct their processing.
Frequency	Continuous, for the duration of the live Programs.

Annex B. Technical and Organizational Measures

The technical and organizational measures are those set out in the Security Measures (Schedule 2), in the version referenced in the Order Form.

Annex C. Authorized Sub-processors

SUB-PROCESSOR	PURPOSE	LOCATION
Amazon Web Services (AWS)	Cloud hosting and infrastructure	Singapore

SUB-PROCESSOR	PURPOSE	LOCATION
Twilio Segment	Data pipeline	EU
CleverTap	CRM and consumer engagement	USA
Microsoft	Power BI reporting and analytics	EU
Vonage B.V.	SMS and WhatsApp messaging, one-time password processing	Netherlands
OpenAI (enterprise)	AI-assisted receipt and product image processing	USA
Google (Gemini, enterprise)	AI-assisted receipt and product image processing	USA
Anthropic (enterprise)	AI-assisted receipt and product image processing	USA
Yoti Ltd	Age verification (facial age estimation or identity document check), only for Programs where it is ordered	United Kingdom
Tremendous	Digital reward fulfilment (gift cards, prepaid cards, vouchers) and redemption fraud checks	USA

The AI model providers receive only the submitted image, under enterprise API terms that exclude the use of inputs and outputs for model training; no other Campaign Participant Data is transmitted to them. Tremendous receives, through Provider's API integration, only the Campaign Participant's email address or phone number, together with the reward details, which it uses to deliver the reward and to verify the redemption against fraud. Details a Campaign Participant enters on its redemption page (such as payout details) are collected by Tremendous under its own terms and privacy notice. Changes to this list follow Section 5.2.

Annex D. Joint Controller Arrangement (Art. 26 GDPR)

ITEM	ALLOCATION
Scope	Campaign Participant Data of Programs whose mechanics are recorded as co-designed in the Order Form or the Program brief (Section 2.1).

ITEM	ALLOCATION
Transparency	Provider makes the End-User Documentation available to data subjects at account creation and Program opt-in. Client is responsible for the accuracy of its Program terms and for its own privacy notices covering its use of the data it receives.
Legal basis and consent	Consent to Program participation and to Client's communications is captured through the Platform opt-in flow and recorded in Provider's consent management service, including the version of the documents accepted. Client is responsible for the lawfulness of its own subsequent marketing to opted-in consumers.
Data subject rights	The Platform self-service tools and privacy@wecheer.io are the primary contact point for data subjects. Provider handles access, rectification and deletion requests at Platform level; Client handles requests relating to data it has received into its own systems. Each Party forwards relevant requests to the other without undue delay. Data subjects may exercise their rights against either Party.
Security	Provider is responsible for Platform security under Annex B; Client is responsible for the security of data exported to or received in its own systems, including through data routers.
Breach	Each Party notifies the other without undue delay (Provider: within 48 hours) of a breach affecting jointly controlled data. The Party in whose environment the breach originated leads notifications to regulators and data subjects, in coordination with the other.
Information to data subjects	A summary of this arrangement is available to data subjects on request at privacy@wecheer.io.