WECHEER LEGAL

General Terms & Conditions

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

These general terms and conditions (**GTC**) form, together with any order form signed or accepted by the Parties that references them (**Order Form**) and the schedules listed in Section 20 (**Schedules**), a legal agreement (**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**, and together with Provider, the **Parties**).

1. Scope

1.1 In General. These GTC govern Client's rights and obligations with respect to the services detailed in the Order Form (the **Services**), including access to the Wecheer platform (the **Platform**) with the functionalities, modules, allowances and limitations specified in the Order Form, whose prices and allowances, together with any rate card it references, form the **Rate Card**.

1.2 No Further Obligation. Provider has no obligation to provide any service or software that is not expressly specified in these GTC or in the Order Form.

1.3 Programs. The Services are provided per Program. A **Program** is one experience on the Platform that serves one type of user (for example consumers, or retail and trade staff), for one brand or brand group, with one mechanic, under one set of participation terms and one opt-in. Within a Program, Client may make unlimited changes to creative, rewards and prizes, and add products of the same brand or brand group. A change of user type, brand group, mechanic or opt-in creates a new Program. A Program is live in a calendar month if it is open to Campaign Participants on any day of that month.

2. Acceptance and Order Forms

2.1 Acceptance. Client accepts these GTC by signing an Order Form, including by electronic signature, or by accepting an Order Form online in accordance with Section 18.8.

2.2 Applicable Version. The version of these GTC and of each Schedule that applies to Client is the version referenced in the Order Form, as published by Provider at the address stated in the Order Form. Later versions apply only in accordance with Section 18.4.

2.3 Changes Without a New Order Form. During the Term, Client may, by email from its Order Form contact or through the Platform where available: add or remove Programs; raise the monthly usage ceiling; and order any other item priced in the Rate Card. Such changes are billed at the rates of the Rate Card and require no new Order Form. Programs and services ordered in the Order Form cannot be reduced below the ordered quantity during the Commitment Period or minimum period. A new Order Form is required for a change of plan, a new market, any item not priced in the Rate Card, or a renewal on different terms.

3. Services

3.1 In General. Subject to Client's compliance with the Agreement, in particular the payment of the Fees in accordance with Section 10, Provider provides the Services specified in the Order Form. Services may include, if and to the extent provided in the Order Form: (i) program design, campaign management, consultancy or advisory services; (ii) provision of the Platform pursuant to Section 4; (iii) Maintenance Services and Support Services pursuant to Section 5; and (iv) any additional services described in the Order Form or ordered under Section 2.3.

3.2 Obligation of Means. Provider supplies the Services under an obligation of means, in accordance with standard professional practice, with the care and diligence required from a supplier of similar services.

3.3 Planning. Provider endeavours to supply the Services within the deadlines set out in the Order Form. Deadlines are indicative unless the Order Form expressly states that they are binding.

3.4 Changes. Provider may implement modifications to the Licensed Products, including to their layout or functionalities, and may remove Content from the Platform or change its functionalities, provided that such modifications do not materially degrade the functionality or availability of the Services for a live Program.

4. Platform and Licensed Products

4.1 In General. During the Term, Provider makes the Platform and the content displayed on, or generated through, the Platform or the Services (the **Content**, and together with the Platform, the **Licensed Products**) available to prospective or current customers, consumers or trade users of Client (the **Campaign Participants**) participating in Client's Programs.

4.2 End-User Documentation. Access to and use of the Platform by any Campaign Participant requires the prior acceptance of the Platform's terms of use and privacy notice, in their form available from time to time on the Platform (**End-User Documentation**). Client complies, and causes its authorized users to comply, with the End-User Documentation and with any reasonable guidelines Provider issues for the use of the Licensed Products.

4.3 Access to Content by Client. Provider makes the Content, dashboards, reports and data exports of Client's Programs available to Client in the Platform's back office, and provides any further reports specified in the Order Form. Any Licensed Products made available to Client are licensed under a revocable, non-exclusive and non-transferable right to use for Client's internal business purposes only, in accordance with these GTC and the End-User Documentation, and are not assigned to Client. Client has no right to access the source code of, modify, copy, reproduce or prepare derivative works based on the Licensed Products, unless the Order Form expressly provides otherwise.

4.4 No Delivery. The Licensed Products are provided as software as a service. Provider grants Client a right to access and use the Licensed Products and delivers no copy of them.

4.5 Developments. Any customization, additional feature, patch, bug fix, update or upgrade of the Licensed Products made available by Provider in connection with the Services (**Developments**) automatically becomes part of the Licensed Products, unless otherwise stipulated by Provider.

4.6 APIs and Integrations. During the Term, Provider maintains the Platform's inbound and outbound application programming interfaces (APIs) and webhooks, together with their documentation. Any change to an API that is not backward compatible is notified to Client at least thirty (30) days in advance, except where a shorter period is required for security reasons or by a third-party provider. Integrations between the Platform and Client's systems are built by Provider, at the rates of the Rate Card or as quoted in the Order Form.

4.7 AI Functions. Where selected, the Platform's AI-assisted purchase validation functions (Receipt Scanning and Snap & Earn) and their supporting checks (the **AI Functions**, as defined in Schedule 1) are provided on the terms of Schedule 1. Where they are not selected, purchase validation in Client's Programs uses unique codes, QR codes or other methods that do not involve those functions.

---

5. Availability, Maintenance and Support

5.1 Availability. Provider uses commercially reasonable endeavours to maintain the availability of the Licensed Products. The availability target and support levels are set out in the Support Policy (Schedule 5). Service credits apply only where a service level agreement is expressly included in the Order Form.

5.2 Maintenance Services. Provider continuously seeks to identify and resolve problems that may negatively affect the proper functioning and availability of the Licensed Products (**Maintenance Services**). Maintenance Services comprise repairs (rectification of faults and errors to restore functionality) and servicing (maintenance to maintain functionality). Further development, adaptation or improvement of the Licensed Products does not form part of the Maintenance Services.

5.3 Maintenance Windows. As a rule, Maintenance Services are deployed once a week during maintenance windows (weekdays between 18:00 and 09:00 CET, or during the weekend), for no longer than one hour, during which the Licensed Products may be fully or partly unavailable. Provider informs Client reasonably in advance where maintenance has to be performed outside these windows or is expected to cause unavailability of more than one hour.

5.4 Support Services. Provider provides technical support for the notification and correction of defects or errors affecting the Platform (**Support Services**) in accordance with the Support Policy (Schedule 5).

---

6. Client's Obligations

6.1 Payment of Fees. Client pays the Fees in accordance with Section 10.

6.2 Proper Use. Client complies at all times with all laws and regulations applicable to its use of the Services and to the provision of the Licensed Products to Campaign Participants, and with the conditions and limitations of any right granted under the Agreement. In particular, Client shall not, without Provider's prior written consent, during or after the Term: (i) use the Services for any illegal purpose; (ii) republish or redistribute any Content or material from the Licensed Products, other than as intended for its Programs; (iii) use the Services or Provider's infrastructure to build a competing product or service or to copy their features or user interface; or (iv) license, sell, rent, lease, transfer, assign, distribute, disclose or otherwise make the Services or the Licensed Products available to any third party, or use them on behalf or for the benefit of any third party, other than as part of the operation of its Programs.

6.3 Licenses and Authorizations. Client maintains all permits and licenses required for its use of the Services in the territories where it operates or where its Programs are available.

6.4 Point of Contact. Client designates in the Order Form a reliable point of contact who provides feedback and up-to-date information on Client's business as reasonably required for the Services.

6.5 Assistance. Client provides Provider with the assistance and information reasonably required for the proper performance of the Services.

6.6 Program Responsibilities. Client is responsible for: (a) the rules and participation terms of its Programs, including any prize, promotion or reward terms, and their compliance with the laws of each market where a Program is available, including laws on promotions, prize draws, lotteries and consumer protection; (b) the content, brand assets, product data and other materials it provides, and its right to use them; (c) funding the rewards of its Programs; (d) age restrictions and other rules applying to its product category, including for alcohol, tobacco, nicotine and other regulated products; and (e) its own marketing to Campaign Participants who have opted in to receive it. Provider configures the Platform according to Client's instructions and may decline any configuration it reasonably considers unlawful.

6.7 Client Default. Where Client fails to comply with its obligations under the Agreement, Provider is excused from the performance of its obligations to the extent affected and assumes no liability in that respect, without prejudice to Provider's other rights.

---

7. Client Materials

7.1 Ownership. Client may provide Provider with documents, information and other data in connection with the Services (**Client Materials**). Subject only to Section 7.2, Client Materials remain, as between the Parties, the sole and exclusive property of Client, and nothing in the Agreement transfers ownership of any Client Materials to Provider.

7.2 Use of Client Materials. Client grants Provider a worldwide, royalty-free, non-exclusive license to use the Client Materials for the sole purpose of providing and improving the Licensed Products and the Services, including the calibration and optimisation of the Platform's validation and fraud-prevention functions on Client's Program data during the Term, and including a license to collect, process, store, generate, anonymize and modify the Client Materials and to transfer them to subcontractors engaged in the provision of the Services that are bound by confidentiality and data protection obligations at least as protective as those of the Agreement. This license terminates on termination of the Agreement, except for Client Materials that have been irreversibly anonymized or aggregated. Provider does not sell or otherwise commercialize the Client Materials.

7.3 Fraud Prevention. To protect the integrity of Programs across the Platform, Provider processes fraud signals derived from submissions (such as hashes of receipt and product images, device and network identifiers, code usage and submission patterns) at Platform level, in order to detect duplicate, manipulated or fraudulent submissions across Programs and clients. No Client Materials, Program content or Campaign Participant identity is disclosed to any other client through this processing.

7.4 Warranty. Client warrants that (i) it has valid grounds and, where required, all authorizations and consents for the processing of the Client Materials under the Agreement, and (ii) the Client Materials do not infringe any law, regulation or third-party right. Provider may remove any Client Materials it considers to infringe this warranty.

7.5 Deletion and Return. On termination of the Agreement, Provider provides Client, within a reasonable time following Client's written request, with a final extract of the Client Materials, and then permanently deletes or anonymizes any copies still under its control. Provider may in any case permanently delete or anonymize the Client Materials sixty (60) days after termination or expiry of the Agreement.

---

8. Provider Intellectual Property

8.1 Licensed Products. As between the Parties, Provider is and remains the sole owner of all rights, title and interest, registered or not, in copyright, databases, trademarks, domain names, designs, patents, know-how, business secrets and all other intellectual property or similar proprietary rights of whatever nature (**Intellectual Property Rights**) in and to the Services and the Licensed Products, including any Development, but excluding the Client Materials. Nothing in the Agreement assigns or transfers any Intellectual Property Rights to Client.

8.2 Usage Data. Provider owns and may freely use, including for benchmarking, analytics and the development of its services, data (i) collected through cookies or other tracking and analytics technology on the Platform, (ii) relating to Client's and Campaign Participants' access to and use of the Licensed Products, and (iii) derived from user inputs, provided that reasonable efforts are made to remove any reference to Client and to identifiable individuals (**Usage Data**). Usage Data consists of aggregated or de-identified information and does not include personal data of Campaign Participants, whose processing is governed by Section 11 and the DPA. Nothing in this Section limits Client's right to the Program data, reports and Content described in Section 4.3.

8.3 Notice of Infringement. Client informs Provider without delay of any actual or threatened infringement of Intellectual Property Rights in the Services or the Licensed Products of which it becomes aware. Provider has the exclusive power to decide on any action to be taken, and Client provides reasonable assistance at Provider's request and cost.

8.4 Third-Party Claims. If Provider is enjoined from providing the Services or Licensed Products because of a third-party Intellectual Property Rights claim and the injunction is not lifted within thirty (30) days, or if a final court decision finds that Client's permitted use of the Services or Licensed Products infringes third-party Intellectual Property Rights, Provider at its expense either (a) obtains for Client the right to continue using them, (b) modifies or replaces them so that they no longer infringe, or (c) where Provider reasonably considers (a) and (b) commercially unreasonable, terminates the Agreement with immediate effect and refunds any prepaid Fees for the period of non-use. This is Client's sole and exclusive remedy for such claims.

8.5 Relief. Client acknowledges that any infringement of Provider's Intellectual Property Rights causes irreparable harm to Provider, for which monetary damages alone would be inadequate, and that Provider may seek injunctive relief or any other remedy available in any jurisdiction.

---

9. Third-Party Components

9.1 In General. The Services or Licensed Products may include or require content or software components developed, distributed or licensed by third parties (**Third-Party Components**). Client uses Third-Party Components in accordance with the applicable third-party terms.

9.2 Main Third-Party Terms. Depending on the features used in a Program, the following third-party terms apply: WhatsApp Business messaging (Meta's WhatsApp Business terms and policies, including template approval, opt-in and content rules); SMS (applicable carrier and country rules for application-to-person messaging); messaging delivery (Vonage terms of service); age and identity verification, where ordered (Yoti terms); digital rewards (the terms of Provider's reward platform, Tremendous, and the redemption terms of the relevant voucher or gift card issuer); and AI-assisted validation (the enterprise API terms of the AI model providers listed in the DPA). Provider provides current links to these terms on request.

9.3 Open Source. Nothing in these GTC restricts or otherwise affects any rights or obligations Client may have under the open source licenses of any open source software included in or provided with the Licensed Products.

---

10. Fees, Billing and Payment

10.1 Fees. Client pays the fees set out in the Order Form and, for items billed on use, the rates of the Rate Card (the **Fees**), in the currency of the Order Form.

10.2 Calendar Months. Billing follows calendar months. Every Order Form starts on the first day of a calendar month (the **Start Date**). Fees are not prorated.

10.3 One Monthly Invoice. On the first day of each month, Provider issues one invoice covering: (a) the fixed Fees for that month (licence, Programs and add-on services ordered in the Order Form), in advance; and (b) the variable Fees for the previous month (additional Programs added under Section 2.3, usage above the allowances of the Order Form, messaging, age and identity checks, rewards sourced by Provider and any other item billed on use), in arrears. Usage is visible in the Platform during the month.

10.4 Payment. Invoices are due on receipt. Unless the Order Form provides for payment by bank transfer, Client registers a payment method (direct debit or card) with Provider's payment service provider when entering into the Order Form, and authorizes Provider to collect each invoice from that payment method on its due date. Client keeps a valid payment method on file for the whole Term. Payment details are held by the payment service provider and are not stored by Provider.

10.5 No Refund. Fees paid are not refundable, including on termination or expiry of the Agreement, except as expressly provided in these GTC.

10.6 Monthly Usage Ceiling. Variable Fees are subject to the monthly ceiling stated in the Order Form. Provider alerts Client's contact by email when 80% of the ceiling is reached in a month. At 100%, non-transactional messaging and further volumes above the allowances pause until Client raises the ceiling, by email or in the Platform. One-time passwords, transactional messages and live Programs are never paused.

10.7 Rewards Sourced by Provider. Where Client asks Provider in writing to source rewards, the reward value and the sourcing fee are charged as set out in the Rate Card. Provider may require Client to prefund part or all of the approved reward budget before procurement; otherwise the reward value is billed with the monthly variable Fees, and redemptions of Provider-sourced rewards pause when the reward ceiling stated in the Order Form is reached in a month.

10.8 Taxes. Fees are exclusive of all taxes, duties, levies and similar charges of any kind, in particular VAT, which are borne by Client where applicable. Swiss VAT is added for Clients established in Switzerland; Clients established elsewhere account for any VAT or similar tax under the reverse-charge mechanism where applicable. All payments are made free and clear of any deduction or withholding; if Client is required by law to deduct or withhold any tax, the amount payable is increased so that Provider receives the full amount it would have received without such deduction or withholding.

10.9 Late Payment and Suspension. If a collection fails, the payment service provider retries it. If an amount remains unpaid fourteen (14) days after its due date, Provider may suspend Client's access to the Platform's back office. If an amount remains unpaid thirty (30) days after its due date, Provider may suspend the Services, including live Programs, and terminate the Agreement for cause. Overdue amounts bear default interest at five percent (5%) per year, and Client bears the reasonable costs of collecting them. A reversed direct debit or a card chargeback counts as non-payment from the date of the reversal, and Client bears the related fees. Where collections have failed more than once, Provider may require the following months to be paid in advance by bank transfer.

10.10 Changes to Fees. On a flexible plan, Provider may change the Fees with sixty (60) days' notice by email; Client may then terminate by written notice effective on the date the change applies, notwithstanding Section 17.3 and any minimum period. On a committed plan, the Fees are fixed for the Commitment Period; changes apply from the next renewal and are notified at least sixty (60) days before the end of the Commitment Period. Messaging and other third-party pass-through rates are not fixed: they follow the list published by Provider when the usage occurs.

---

11. Data Protection

11.1 DPA. The processing of personal data under the Agreement is governed by the Data Processing Agreement (Schedule 4, the **DPA**). In case of conflict between these GTC and the DPA with respect to personal data, the DPA prevails. Provider's privacy notice, published on its website, describes how personal data is collected through the Platform.

11.2 Roles. The roles of the Parties for each category of personal data are set out in Section 2 of the DPA. Provider does not sell personal data of Campaign Participants and does not use it for third-party advertising.

11.3 Client's Obligations. Client ensures that any personal data it provides to Provider has been collected and transferred in compliance with applicable data protection laws, and in particular that it has and maintains valid grounds for the processing it instructs.

11.4 Compliance Actions. Unless prohibited by law, Provider may forward to Client any request, investigation or other action of a supervisory authority or third party, including a data subject, relating to personal data processed on Client's behalf. Where Provider has to take compliance action itself or assist Client beyond the assistance included in the DPA, Client reimburses Provider's reasonable costs.

---

12. Confidentiality

12.1 Definition. Confidential Information means any information disclosed by one Party (the **Disclosing Party**) to the other (the **Receiving Party**), directly or indirectly, in writing, orally or by inspection, that is designated as confidential or can reasonably be considered confidential. It includes the content of the Agreement (but not the fact that the Parties work together) and all information about the Disclosing Party's business and operations. The Licensed Products, the Services and Usage Data are Confidential Information of Provider. Confidential Information does not include information that: (i) was public before disclosure; (ii) becomes public through no act or omission of the Receiving Party; (iii) was already in the Receiving Party's possession, as shown by its records; (iv) is obtained from a third party without breach of confidentiality; or (v) is independently developed by the Receiving Party without use of the Confidential Information.

12.2 Obligation of Confidentiality. The Receiving Party does not disclose, sell, license, transfer or otherwise make available the Disclosing Party's Confidential Information to any person, except to its employees, agents, subcontractors and advisers who need to know it to perform the Agreement and are bound by equivalent obligations, and does not use it except to perform the Agreement.

12.3 Return. On the Disclosing Party's written request, the Receiving Party returns or deletes the Disclosing Party's Confidential Information.

12.4 Legal Disclosure. The Receiving Party may disclose Confidential Information where required by law or by a court or authority, provided that it gives the Disclosing Party prompt notice where permitted and limits the disclosure to what is required.

12.5 Feedback. Provider may freely use any suggestion or idea for improving its products or services that Client provides (**Feedback**), without compensating or crediting Client.

---

13. Publicity

Provider may refer to Client as a customer, and use Client's name and logo for that purpose in its marketing materials, with Client's prior written consent, which shall not be unreasonably withheld. Client grants Provider, during the Term, the licenses needed to display Client's names, logos, trademarks and Program assets within the Platform and its Programs.

---

14. Limited Warranty

14.1 As Is, As Available. The Services and the Licensed Products are provided as is and as available. To the maximum extent permitted by law, Provider disclaims all warranties, whether express, implied or statutory, including any warranties of merchantability, fitness for a particular purpose, quiet enjoyment and non-infringement.

14.2 Exclusions. In particular, Provider does not warrant that the Services or Licensed Products will meet Client's requirements, operate without interruption or error, remain compatible with third-party products, remain available unchanged, or that a given plan will remain available for renewal. Provider gives no warranty regarding any decision Client takes on the basis of insights from the Services.

---

15. Limited Liability

15.1 Limitation. Provider's liability under the Agreement, whether in contract, tort or any other theory, is excluded and limited to the maximum extent permitted by law. Nothing in the Agreement excludes or limits liability for gross negligence or willful misconduct, or any other liability that cannot be excluded or limited by law.

15.2 Excluded Damages. To the extent permitted by law, Provider is not liable for simple negligence, nor for loss of use, interruption of business, loss of profit, revenue, savings, opportunity, goodwill or reputation, loss or corruption of data, or any indirect, special, incidental, exemplary or consequential damages.

15.3 Cap. Provider's total liability in any period of twelve (12) months does not exceed the Fees actually paid by Client in the twelve (12) months preceding the event giving rise to the claim.

15.4 Auxiliaries. The exclusions and limitations of this Section 15 also apply to Provider's directors, officers, employees, agents, representatives and auxiliaries.

16. Indemnification

16.1 Indemnity. Client defends, holds harmless and indemnifies Provider and its directors, officers, employees and auxiliaries from and against all liability, loss, cost, damage or expense, including reasonable legal fees, arising from: (i) Client's use of the Services or Licensed Products other than as permitted by the Agreement; (ii) Provider's use of the Client Materials as permitted by the Agreement; or (iii) the rules, prizes, rewards and content of Client's Programs, including any claim that they breach the laws referred to in Section 6.6.

16.2 Procedure. Provider informs Client without undue delay of any claim covered by Section 16.1 and allows Client to assist in its defence and settlement with counsel of Client's choosing and at Client's expense, where procedural rules permit.

17. Term and Termination

17.1 Entry into Force. The Agreement enters into force on the earlier of the signature or online acceptance of the Order Form and Client's first use of the Services.

17.2 Plans. The Order Form states Client's plan: (a) on a **committed plan**, the commitment period is twelve (12) months from the Start Date (the **Commitment Period**); (b) on a **flexible plan**, the minimum period is three (3) months from the Start Date, after which the plan continues month to month. The fixed Fees for the whole Commitment Period or minimum period are due, even if Client stops using the Services earlier, and continue to be collected monthly.

17.3 Renewal and Notice. A committed plan renews automatically for successive Commitment Periods of twelve (12) months, unless either Party gives written notice at least thirty (30) days before the end of the current Commitment Period. After its minimum period, a flexible plan continues until either Party terminates it with at least thirty (30) days' written notice, effective at the end of a calendar month. The initial period and any renewal together form the **Term**.

17.4 Termination for Cause. Provider may terminate the Agreement with immediate effect in case of material breach by Client, including under Section 10.9; where the breach can be cured, Provider first gives Client twenty (20) days' written notice to cure it, except for termination under Section 10.9, to which no further cure period applies. Provider may also terminate the Agreement where Client's use of the Services infringes, or risks infringing, third-party rights. Client may terminate the Agreement in case of material breach by Provider that remains uncured thirty (30) days after Client's written notice describing the breach.

17.5 Effects of Termination. On termination or expiry: (a) Provider stops providing and Client stops using the Services and Licensed Products; (b) all access rights and credentials are deactivated; (c) each Party returns or deletes the other's Confidential Information, at the Disclosing Party's option; and (d) Fees already paid remain acquired to Provider, and Client immediately pays all outstanding amounts and, where Provider terminates for cause, the fixed Fees for the remainder of the Commitment Period or minimum period, which become due at once.

17.6 Survival. Provisions that are expressed or intended to survive, and those necessary to interpret or enforce the Agreement, survive its termination or expiry.

18. Miscellaneous

18.1 Independent Contractors. The Parties are independent contractors. Neither Party has authority to bind the other, and neither holds itself out as the other's agent, employee, joint venturer or partner.

18.2 Subcontractors. Provider may use subcontractors for the provision of the Services and remains responsible for their performance.

18.3 Force Majeure. Neither Party is liable for any delay or failure to perform caused by events beyond its reasonable control, such as natural disasters, war, strikes, power or internet failures, epidemics or similar events, for as long as the event lasts. The affected Party notifies the other promptly, uses its best efforts to limit the delay, and informs the other of its plans to resume performance.

18.4 Changes to these Documents. Provider may publish new versions of these GTC and the Schedules. A new version applies to Client: (a) on a flexible plan, thirty (30) days after Provider notifies it by email, Client being entitled to terminate by written notice effective on that date, notwithstanding Section 17.3 and any minimum period; and (b) on a committed plan, from the next renewal. Changes to the list of sub-processors follow the procedure of the DPA. The Order Form may be amended only in writing, signed or accepted by both Parties, or as permitted by Section 2.3.

18.5 Entire Agreement. The Agreement, together with the End-User Documentation, is the entire agreement between the Parties on its subject matter and supersedes all prior representations, understandings and agreements. Terms in Client's purchase orders or vendor documents do not apply, even if accepted or signed by Provider.

18.6 Order of Precedence. In case of conflict: the DPA prevails for the processing of personal data; Schedule 1 prevails for the AI Functions; otherwise these GTC prevail over the Order Form and the other Schedules, unless the Order Form expressly deviates from a section of these GTC that it cites.

18.7 Severability. If a provision of the Agreement is held invalid or unenforceable, the Parties replace it with a valid provision that reflects their original intent as closely as possible. All other provisions remain in force.

18.8 Electronic Signature and Online Acceptance. Signature includes electronic signatures (such as DocuSign or an equivalent provider) and the online acceptance of an Order Form through a process that records the name, email address and title of the accepting person, the date and time, and the versions of the documents accepted. Both have the same legal effect as a handwritten signature. "In writing" includes email.

18.9 Notices. Notices are sent by email to the contacts stated in the Order Form, or to any other address a Party notifies to the other.

18.10 No Waiver. A Party's failure to require performance of any obligation does not affect its right to enforce it later.

18.11 Assignment. Neither Party may assign or transfer the Agreement, in whole or in part, without the other's prior written consent. Provider may however, without Client's consent: (i) assign the Agreement to a third party acquiring all or substantially all of its business related to the Services; and (ii) assign, pledge or otherwise transfer its rights to payment under the Agreement, including for factoring or other financing purposes.

18.12 No Third-Party Beneficiaries. Except under Section 16, the Agreement confers no rights on any third party.

---

19. Governing Law and Jurisdiction

19.1 Governing Law. The Agreement and any use of the Licensed Products are governed by Swiss substantive law, excluding its conflict of laws rules and the United Nations Convention on Contracts for the International Sale of Goods.

19.2 Jurisdiction. The ordinary courts of Lausanne, Switzerland, have exclusive jurisdiction over any dispute arising out of or in connection with the Agreement. Provider may in any case seek injunctive relief in any jurisdiction to protect its Intellectual Property Rights.

---

20. Schedules

The following Schedules, in the version referenced in the Order Form, form part of the Agreement:

- **Schedule 1:** Artificial Intelligence
- **Schedule 2:** Security Measures
- **Schedule 3:** Rate Card: the prices and allowances of the Order Form and any rate card it references, including the messaging unit costs published at wecheer.io/pricing/messaging-costs
- **Schedule 4:** Data Processing Agreement
- **Schedule 5:** Support Policy

SCHEDULE 1 TO THE GTC

Artificial Intelligence

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

This Schedule sets out the terms on which Provider uses artificial intelligence to validate purchases in Client's Programs. Capitalized terms not defined here have the meaning given in the GTC. In case of conflict with the GTC, this Schedule prevails for the AI Functions.

1. AI Functions

1.1 Scope. This Schedule covers the following functions of the Platform (the **AI Functions**):

- **Receipt Scanning:** AI-assisted reading of purchase receipts submitted by Campaign Participants, to extract the retailer, date, products and amounts needed to validate a purchase.
- **Snap & Earn:** AI-assisted recognition of a product or pack photographed by a Campaign Participant, to validate a purchase or consumption without a receipt.
- **Image authenticity and fraud checks:** the checks that support these two functions, such as live-capture controls and the detection of duplicate, manipulated or AI-generated images.

1.2 Client's Choice. Client selects the validation methods in the Order Form or, for Programs added under Section 2.3 of the GTC, in the change request. Where Client selects Receipt Scanning or Snap & Earn, it approves the use of the AI Functions for that Program on the terms of this Schedule. Where neither is selected, validation uses unique codes, QR codes or other methods, and no Client Materials are processed by the AI Functions.

2. How the AI Functions Work

2.1 Model Providers. The AI Functions combine Provider's own validation logic with AI models from the providers listed in Annex C of the DPA, used under their enterprise API terms, which exclude the use of inputs and outputs to train their models. Provider may move between the model providers listed there without further approval; new providers follow the sub-processor procedure of the DPA.

2.2 Data Sent. Only the image submitted by the Campaign Participant is sent to the model providers. No name, contact detail or other identifier of the Campaign Participant is transmitted with it.

2.3 Adaptive Validation. Receipt Scanning and Snap & Earn are adaptive: their accuracy on Client's products and retailers, and their resistance to fraud, improve as they process Client's Program data. Client agrees that Provider calibrates and optimises the AI Functions on that data during the Term, in accordance with Sections 7.2 and 7.3 of the GTC. Client Materials are not disclosed to other clients.

2.4 Human Oversight. Provider's operations team monitors validation outcomes, reviews flagged or contested submissions and can override an automated decision. Campaign Participants can contest a validation decision through the support channel of the Platform.

2.5 Transparency. The End-User Documentation informs Campaign Participants that AI assists the validation of their submissions.

3. Commitments

3.1 Regulatory Assessment. Provider has assessed that the AI Functions are not a prohibited practice, a high-risk AI system or a general-purpose AI model under Regulation (EU) 2024/1689 (the EU AI Act). Provider informs Client without undue delay if this assessment changes.

3.2 Security. The AI Functions are covered by the Security Measures (Schedule 2) and the DPA.

3.3 Accuracy. The AI Functions are designed and monitored to validate purchases reliably, but automated reading and recognition can contain errors. Validation thresholds and review rules are set with Client during Program design. Provider's liability for the AI Functions is governed by the GTC.

3.4 Information. Provider's Position Statement on the Use of Artificial Intelligence is available to Client on request, together with any further information Client reasonably needs to assess the AI Functions or to meet its own obligations under applicable AI laws.

SCHEDULE 2 TO THE GTC

Security Measures

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

This Schedule describes the technical and organizational measures Provider maintains to protect the Platform and the data processed through it. It also forms Annex B of the Data Processing Agreement (Schedule 4). Provider reviews these measures at least once a year and may update them, provided the overall level of protection is not reduced. Further detail, including penetration test summaries and security policies, is available to Client on request under confidentiality, as set out in Section 10 of the DPA.

Measures

AREA	MEASURES
Framework	Information security programme aligned with ISO/IEC 27001 and 27002, with security, asset management and data protection policies approved by management. The Platform is hosted on Amazon Web Services, whose infrastructure is ISO/IEC 27001 certified.
Encryption	Data encrypted in transit (TLS 1.2 or higher) and at rest (AES-256), including backups.
Access control	Role-based access on a least-privilege, need-to-know basis, reviewed periodically. Multi-factor authentication on administrative access. Personal credentials only. Access removed promptly when no longer needed.
Infrastructure	Cloud-native architecture on managed cloud services. Logical segregation of each client's data on the shared Platform. Data stores not exposed to the public internet. Public endpoints protected against abuse.
Application security	Authenticated, rate-limited APIs over HTTPS. Secure development practices, including code review, dependency management and automated code analysis.
Testing	Regular independent security assessments of the production Platform, and a penetration test by an independent third party at least once every 12 months. Findings prioritised by severity and remediated.

AREA	MEASURES
Monitoring	Security-relevant events on production systems logged and monitored. Administrative actions on the infrastructure recorded.
Backup and recovery	Encrypted automated backups, retained for up to 30 days. Restoration tested at least once a year.
Incident management	Documented incident response process covering identification, containment, notification and post-incident review. Personal data breaches notified to Client within 48 hours, as set out in Section 8 of the DPA.
Personnel	Confidentiality obligations for personnel and contractors. Information security training at least once a year. Approved devices and an acceptable use policy.
Data minimization and deletion	Consumer self-service account deletion, with a 30-day dormancy period, then permanent deletion or anonymization. Program-level deletion on Client's instruction. Aggregation and anonymization for analytics. Retention and deletion as set out in Section 9 of the DPA.
Sub-processors	Security due diligence before engagement. Written obligations at least as protective as this Schedule. List and locations in Annex C of the DPA.

SCHEDULE 4 TO THE GTC

Data Processing Agreement

Version 2026-10 Published 18 October 2026, updated 19 October and 5 November 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 results (pass or fail against the age required for the Program), only where age verification is ordered. The facial image or identity document used for the check is captured and processed directly by the age verification sub-processor listed in Annex C; it is not transmitted to, received or stored by Provider.
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
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. The check runs in Yoti's own interface, and Yoti returns only the result (pass or fail) to Provider	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).
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.

SCHEDULE 5 TO THE GTC

Support Policy

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

This Support Policy sets out how Provider supports Client and keeps the Platform available. It applies to all Services, unless the Order Form includes a service level agreement, in which case that agreement applies instead. Capitalized terms not defined here have the meaning given in the GTC.

1. Support Channels and Hours

1.1 Channels. Client reports incidents and requests to its Customer Success Manager and to support@wecheer.io. Each report states the Program concerned, what happened, when, and, where possible, screenshots or examples.

1.2 Hours. Support is available on business days from 09:00 to 18:00 in Client's time zone, as stated in the Order Form, provided by Provider's teams in Asia, Europe and the Americas.

2. Availability Target

Provider targets a monthly availability of 99.5% for the core consumer journey: the ability of Campaign Participants to open the Wecheer application, join a Program, submit a validation (receipt, product image, QR code or link) and redeem an available reward. Scheduled maintenance within the windows of Section 5.3 of the GTC, pauses at the usage or reward ceiling under Sections 10.6 and 10.7 of the GTC, force majeure, failures of third-party channels outside Provider's control (such as WhatsApp, SMS carriers, email providers, reward suppliers and app stores) and suspensions permitted by the Agreement are excluded. This is a target: no service credits apply.

3. Incident Priorities

Client indicates the priority when reporting an incident; Provider may reclassify it in line with the definitions below. Response means acknowledgment and start of qualified work. Resolution means restoring the affected function or providing an acceptable workaround; a permanent fix may follow in a later release. Times run within the support hours of Section 1.2.

PRIORITY	DEFINITION	RESPONSE	RESOLUTION TARGET
P1, critical	Campaign Participants cannot access the Platform, the Platform is blocked as a whole, data is corrupted, or an essential function of a live Program is blocked without workaround.	1 business hour	8 business hours

PRIORITY	DEFINITION	RESPONSE	RESOLUTION TARGET
P2, major	A non-essential function or business process does not work (for example one mechanic or one messaging channel), a workaround may exist.	8 business hours	8 business days
P3, minor	A defect that does not prevent the use of a function, or degraded performance with an acceptable workaround.	1 business day	15 business days
P4, low	A cosmetic issue, question or change request with no impact on a live Program.	2 business days	Next planned release

Provider works on P1 incidents continuously during support hours, and outside support hours with reasonable efforts where staff are available.

4. Maintenance

Planned maintenance takes place in the windows of Section 5.3 of the GTC. Maintenance expected to cause unavailability outside those windows, or for more than one hour, is announced to Client at least 48 hours in advance, except for urgent security fixes, which are announced as soon as practicable.

5. Escalation

LEVEL	CONTACT	WHEN
1	Customer Success Manager	First contact for all incidents and requests.
2	Head of Technology	A P1 not acknowledged within its response time, or no progress update within four hours.
3	Chief Executive Officer	A P1 unresolved after 24 hours, or repeated misses of the targets of this Policy over three months.

Personal data breaches follow the notification process of the Data Processing Agreement (Schedule 4), which prevails for data protection matters.

6. Customer Success

Program design sessions at onboarding and periodic performance reviews are provided as specified in Section 3 of the Order Form. Configuration changes to live Programs are requested through the Customer Success Manager and scheduled according to their priority.