

Data Processing Agreement (DPA)

Product: REAL Version: 2026.08.09-ENT

Language: English (convenience translation). If this English text conflicts with the Traditional Chinese DPA or a signed Chinese master agreement, the Traditional Chinese version / signed Chinese agreement prevails, unless the parties expressly agree otherwise in writing.

Processor: 艾米亞創意行銷企業社
Contact: amy01058@hotmail.com
Website: https://realvip.cc
Controller (Customer): [Legal name]
Tax ID / Company no.: [] Agreement date: [YYYY-MM-DD]
Effective date: date of signature (or as stated in the Order Form)

This DPA supplements the Master Service Agreement, Order Form, and/or online Terms for use of REAL (the “Service”). If this DPA conflicts with the online Privacy Policy processor terms, this DPA controls; other matters remain governed by the Terms/MSA.

1. Definitions

- “Personal Data” , “collect” , “process” , and “use” have the meanings under Taiwan’ s Personal Data Protection Act (PDPA) and related rules.
- “Customer Personal Data” : personal data submitted, uploaded, generated, or obtained via Third-Party Platforms (e.g. Meta, Google/YouTube) through the Service for the Customer.
- “Instructions” : Customer’ s lawful instructions via Service settings or written/email directions.
- “Subprocessor” : a third party engaged by the Processor to process Customer Personal Data.

2. Roles and scope

- 2.1 For Customer Personal Data, Customer is the collector/controller; Processor processes only under this DPA, Instructions, and Service features.
- 2.2 Purpose: provide social automation, messaging, contacts, analytics, support, security, and platform compliance.
- 2.3 Duration: from Service use / DPA effective date until termination and return/deletion under Section 8 (except legal retention).
- 2.4 Categories (as enabled): identifiers, social IDs, comment/DM content and status, lists/tags, ops/delivery logs, OAuth metadata. Customer shall not instruct processing of sensitive personal data without lawful basis.
- 2.5 Data subjects: Customer staff/agents and End Users interacting with Customer’ s social accounts.

3. Customer obligations

- Ensure a lawful basis to collect/process and to appoint Processor; complete PDPA notices/consents (including indirect collection where applicable).
- Instructions must be lawful; do not require unlawful processing.
- Remain responsible to End Users and authorities as controller; Processor assists within its processor role.
- Manage Account access, offboarding, and internal permissions.

4. Processor obligations

- Process only per Instructions, this DPA, and law; refuse and notify if an Instruction is unlawful.

- Ensure authorized personnel are under confidentiality duties and least privilege.
- Apply risk-appropriate technical and organizational measures (TLS, access control, token protection, logging, incident response).
- Do not sell personal data or use Customer Personal Data for Processor's own unrelated purposes.
- Reasonably assist with data-subject requests, incident notices, and assessments (fees may apply for complex requests).

5. Subprocessors

5.1 Customer provides general authorization for cloud hosting, payments, transactional email/notices, and social platform APIs as needed.

5.2 Processor shall impose contractual protections no less protective than this DPA and remains responsible for subprocessors as permitted by law.

5.3 Main categories: cloud hosting/DB; payments (e.g. Stripe); social platforms (Meta, Threads, Google/YouTube per Customer authorization); transactional email if enabled. Vendors may change; material category changes will be disclosed or notified.

6. Cross-border transfers

Customer Personal Data may be transferred to locations of cloud, payment, or platform providers. Processor will apply PDPA-appropriate safeguards and avoid prohibited transfers. Region-specific restrictions must be stated in an Order Form or annex and agreed in writing.

7. Security incidents

After becoming aware of a personal-data security incident involving Customer Personal Data, Processor will notify Customer within a reasonable period (generally within 72 hours, or sooner if required by law), with known facts, likely impact, and measures taken/planned. Parties will reasonably cooperate.

8. Return and deletion

After termination, disconnect, or Account/Workspace deletion, Processor will return or delete Customer Personal Data (where feasible) and delete remaining copies, except legal, tax, dispute, or backup-rotation retention, after which data will be deleted or anonymized.

9. Audit

Customer may submit one reasonable written questionnaire per year (except urgent incidents). Processor may respond with summaries or questionnaires. Absent a separate written agreement, Processor need not allow on-site audits that would endanger multi-tenant security.

10. Liability and survival

Liability caps, indemnities, and governing law follow the MSA or online Terms unless this DPA says otherwise. Sections 4, 6, 7, 8, 9, 10, and 11 survive termination as applicable.

11. Governing law

Taiwan (R.O.C.) law governs. Negotiate in good faith first; then Taipei District Court has first-instance jurisdiction (unless mandatory consumer rules or a signed master agreement provide otherwise).

12. Signature blocks

[Controller] Legal name: _____ ID: _____ Signatory: _____ Title: _____ Date: _____ Signature/Seal: _____

[Processor] 艾米亞創意行銷企業社 Signatory: _____ Title: _____ Date: _____ Signature/Seal: _____

(Template — complete bracketed fields and obtain counsel review before signing.)