

Privacy Policy — Torro CRM

Operated by Paper Mark Limited ("Torro CRM", "we", "us", "our")

Last updated: 11 August 2026 · Effective: 11 August 2026

Torro CRM is a multi-channel customer-communication platform (CRM) that lets a business manage its conversations from connected messaging channels — including Telegram, WhatsApp, TikTok and (where available) Instagram — in a single inbox, with team collaboration, automation and AI-assisted replies, tasks, and a sales pipeline. This Privacy Policy explains what personal data we process, why, on what legal basis, with whom we share it, how we protect it, and the rights available to individuals.

This policy applies to <https://torrocrm.com> and the Torro CRM application and APIs. It does not apply to third-party services (including the messaging platforms) that have their own privacy policies.

1. Our role: controller and processor

Torro CRM serves two categories of individuals, and our role differs for each:

- **Business users (our customers and their team members).** For personal data about the business account owner and the agents who use Torro CRM (name, email, login, settings, billing), we act as a **data controller**.
- **End-customers (the people a business converses with over a connected channel).** When a business connects a messaging channel and we receive, store and process the messages exchanged with its customers, we act as a **data processor** acting on that business's documented instructions. The business is the **controller** of those conversations and is responsible for having a lawful basis and for informing its end-customers.

Where this policy describes end-customer conversation data, we act as a processor and process it only to provide the service to the relevant business.

2. Data we process

2.1 Business account data (we are controller)

- Identity & contact: name, email address, phone, company/business name, role.
- Account & security: login credentials (stored hashed/encrypted), authentication tokens, security settings.
- Configuration: connected channels, team members and permissions, templates, automations, AI settings.
- Billing: plan, balance, transactions, invoices. Payments are processed by our payment providers (Stripe and Cryptadium); we do **not** store full payment card numbers.
- Usage & technical: IP address, device/browser information, cookies, log and diagnostic data.

2.2 End-customer conversation data (we are processor)

When a business connects a channel, we process, on its behalf:

- **Message content** exchanged between the business and its customers (text, media — images, video, voice notes, files — captions, reactions, delivery/read status).
- **Contact identifiers and profile data** exposed by the channel (e.g. platform username/ID, display name, avatar, phone number where the channel provides it, country).
- **Conversation metadata**: timestamps, which channel/account, assignment, tags/labels, pipeline stage, tasks and notes created by the business's agents.
- **Derived data** produced by our features: transcriptions of voice messages, translations, AI-generated reply suggestions, and message classifications.

We process end-customer data **only for the business that owns the conversation** and only to provide the service.

2.3 Data from connected platforms

Where a business authorizes a channel, we receive data through that platform's official integration:

- **TikTok** — via the **TikTok Business Messaging API**, after the business authorizes our developer app (OAuth). We receive and send the business's Direct Messages and related conversation data for the authorized Business Account only. We do **not** collect public TikTok content and do **not** access TikTok Shop messages.
- **Meta (WhatsApp / Instagram), Telegram**, and other connected channels — analogous, limited to the authorized account's own conversations.

3. How we collect data

- **Directly from business users** — at registration and while using the service.
- **Automatically** — cookies, log data and technical information when the app is used.
- **From connected channels/platforms** — inbound and outbound messages and the associated contact/conversation data, received in real time via the platform's APIs and webhooks after the business authorizes the connection.

4. Purposes and legal bases

Purpose	Data	Legal basis (controller data)
Provide, operate and secure the service	Account, configuration, conversation, usage data	Performance of a contract; legitimate interests
Deliver messaging features (send/receive, inbox, assignment, templates)	Conversation data	Processor — on the business's instructions
AI-assisted features (agent replies, translation, transcription, suggestions)	Message content and derived data	Processor — on the business's instructions (see §5)

Billing and account management	Identity, billing, usage	Performance of a contract
Support, communications, security, fraud/abuse prevention	Account, usage, log data	Legitimate interests; legal obligation
Product analytics and improvement	Aggregated/technical usage data	Legitimate interests

For end-customer conversation data we act as processor; the lawful basis for that processing is the responsibility of the business (controller).

5. AI processing of messages

Torro CRM offers AI-assisted features (an AI agent that drafts/sends replies, automatic translation, voice-message transcription, and content classification). To provide these features, **message content and related context may be processed by third-party AI/LLM sub-processors** (see §7).

We commit that:

- AI processing is performed **only to provide the requested feature** to the business.
- We use, and we select AI sub-processors that contractually commit, **not to use** conversation content **to train foundation/AI models** or for any purpose other than providing the service, and not to retain it beyond what is necessary to deliver the feature.
- Platform data (including TikTok data) is used solely to operate the messaging features and is **never** used for advertising targeting, sold, or shared with unauthorized third parties.

A business can control or disable AI features for its account.

6. Platform compliance and use limitations

Our access to and use of data from TikTok, Meta and other platforms is governed by those platforms' developer terms and policies, in addition to this policy. Specifically, data obtained through a platform integration is:

- used **only** to provide the messaging and CRM features to the authorized business;
- **not** sold, rented, or used for advertising/ad-targeting;
- **not** used to train AI/ML models;
- **not** shared with third parties except the sub-processors strictly necessary to deliver the service (§7);
- **deleted** when the business disconnects the channel or closes the account, or upon a valid deletion request, subject to §9.

For **TikTok** specifically: we only interact with conversations of Business Accounts that have authorized our app; personal (non-business) TikTok accounts are not supported; availability depends on the sign-up region of the Business Account.

7. Sub-processors and third parties

We share personal data only with service providers that process it on our behalf to deliver the service, under contractual confidentiality and data-protection obligations. Categories and current providers:

- **Messaging platforms** (integration counterparties): TikTok / ByteDance, Meta Platforms (WhatsApp, Instagram), Telegram.
- **AI / LLM providers** (for AI agent, translation, transcription): **Eden AI** (which routes requests to underlying model providers under its terms) and **DeepInfra**, selected on the basis that they do not train on or retain customer content beyond providing the feature.
- **Cloud hosting and infrastructure**: hosting located in the **Netherlands and Germany** (servers, database, cache, message queue, search/logging, object storage for media).
- **Payments**: **Stripe** and **Cryptadium**.

We do **not sell** personal data. A current list of sub-processors is available on request.

8. International transfers

Business and conversation data is primarily stored on infrastructure located in the **European Union (the Netherlands and Germany)**. Some sub-processors (for example certain AI or payment providers) may process data in other countries. Where data is transferred across borders, we rely on appropriate safeguards, such as the European Commission's **Standard Contractual Clauses** or an adequacy decision, as required by applicable law.

9. Data retention and deletion

- **Conversation data** is retained while the business keeps the channel connected and its account active, or as instructed by the business, and is then deleted or anonymized within **90 days**.
- **On channel disconnect** we stop processing that channel's data and delete platform-provided data associated with it within **90 days**, except where retention is required by law.
- **On account closure**, we delete or anonymize the business's data within **90 days**, subject to legal retention (e.g. billing records).
- **Data isolation**: each business's data is logically isolated per tenant.
- **End-customer deletion requests**: because we are a processor, requests are routed to and handled by the relevant business (controller); we assist as required.

10. Security

We apply technical and organizational measures appropriate to the risk, including:

- **Encryption in transit** (TLS) and **encryption at rest** for sensitive fields;
- **Multi-tenant logical isolation** so a business can only access its own data;
- **Access controls and least privilege** for staff, with authentication and audit logging;

- Secured EU-based infrastructure, network controls, and monitoring;
- Regular review, vulnerability scanning and penetration testing.

No method of transmission or storage is 100% secure; we work to protect data but cannot guarantee absolute security.

11. Your rights

Depending on your jurisdiction, individuals may have rights to access, correct, delete, restrict or object to processing, and to data portability, and to withdraw consent.

- **Business users** can exercise these rights via account settings or by contacting us (§14).
- **End-customers** should contact the **business** they communicated with (the controller); Torro CRM will support that business in fulfilling the request.

You may also lodge a complaint with your local data-protection authority.

12. Cookies

We use strictly necessary cookies to run the service and, where enabled, analytics/preference cookies. You can control cookies through your browser.

13. Children

The service is intended for businesses and is not directed to children under 16. We do not knowingly collect data from children.

14. Contact

Controller / operator: Paper Mark Limited, Units 1-3, 20F Strand 50, 50 Bonham Strand, Sheung Wan, Hong Kong.

Privacy contact: privacy@torrocrm.com. For privacy questions or to exercise your rights, contact privacy@torrocrm.com.

15. Governing law

This policy is governed by the laws of Hong Kong, without prejudice to mandatory data-protection rights available to individuals under the laws applicable to them.

16. Changes

We may update this policy. Material changes will be notified via the service or by email, and the “Last updated” date will change. Continued use after changes take effect constitutes acceptance where

permitted by law.