TradeRings

LEGAL

TradeRings **Privacy Policy**

VERSION	2.3.1
EFFECTIVE FROM	25 November 2026
SUPERSEDES	TradeRings Privacy Policy v2.3 (17 November 2026)
OPERATOR	TradeRings Corporation, a Florida corporation (document number P24000001413). Registered address: 55 NE 5th Ave, Suite 501, Boca Raton, FL 33432, USA.

What you should know

1. TradeRings records who accepts each legal document by name, device and IP address, and logs which guides and videos each Profile opens, to prove acceptance and to protect the Platform's confidential information (sections 2.6, 2.7, 4.4).
2. The Automated Order Services read incoming order messages and prepare orders, but no order binds anyone until a person confirms it, and you can ask for a human review (section 5).
3. Order details go to your trading counterparties, to the network whose device confirmed the order, to a payment processor you pay through, and to a logistics provider only with the market owner's consent; an originator sees only its own statement (section 6).
4. Acceptance records, guide access logs and watermark traces are kept for the life of the Account and five years after; other information only as long as needed or required by law (section 9).
5. You can ask to access, correct or delete your information at privacy@traderings.io (section 10).

1. About this Policy

TradeRings Corporation ("TradeRings", "we", "us", "our") respects your privacy and is committed to protecting the personal and organisational information of users of the TradeRings trading platform, website, mobile applications, integrations, and related services (collectively, the "Platform").

This Privacy Policy explains what information we collect, how we use it, to whom we disclose it, how we keep it secure, and the rights available to you in relation to it. It sits within the TradeRings legal framework. Acknowledgement of this Privacy Policy is part of the acceptance of the User Terms of Use at Profile registration, and incorporation by reference into the Platform Services Agreement at Account creation. Both documents are available on the Platform.

By accessing or using the Platform, you acknowledge that you have read and understood this Privacy Policy. Where you act on behalf of an organisation (an "Organisation"), you represent that you have authority to bind the Organisation to it.

Defined terms used in this Privacy Policy that are not defined here have the meanings given in the Platform Services Agreement and (for individual-user terms) the User Terms of Use. In particular, an Account may take on the roles of Market Owner, Originator, Network, Activating Account or Logistics Provider, and a Payment Processor is a third party that moves money between buyers and sellers.

2. Information We Collect

2.1 Personal information

We collect personal information that identifies, relates to, or could reasonably be associated with an individual User, including:

1. Full name.
2. Email address.
3. Mobile and other phone numbers.
4. Profile information.
5. Login credentials and authentication factors.
6. Payment information (held by the Payment Processor or card processor concerned, not by TradeRings, where applicable).
7. Records of communications with TradeRings and through the Platform.
8. Usage data within the Platform.
9. Device information and IP address.
10. Identity verification data, where an individual is verified: the verified name and the verification provider's result (verified or not, and the date). The verification provider (currently Sumsub) collects the identity document and the selfie and carries out the face check; TradeRings receives the result, not the document images or the face data.

2.2 Organisation information

We collect information about Organisations that register on the Platform, including:

1. Legal name.
2. Entity type.
3. Registration number.
4. Tax identification number.
5. Registered and trading addresses.
6. Contact details for the Organisation and its Account Owner.
7. Financial information necessary for billing.
8. Trading history and patterns on the Platform.
9. Authorised representatives and their roles.

2.3 Market and Transaction information

We collect detailed information about Markets and Confirmed Orders on the Platform, including:

1. Product details (identifiers, descriptions, units, attachments).
2. Pricing information.

3. Volume and inventory information.
4. Delivery terms (date, location, instructions).
5. Payment terms.
6. The Organisations and Users party to each Confirmed Order.
7. Negotiation and confirmation history.
8. The verified identity of the device on which each Confirmed Order was confirmed, and the Network that device belongs to.
9. Volumetric data (weights and dimensions) and tariff codes carried on Confirmed Orders.
10. Payment Processor outcome records: that a payment was initiated, through which Payment Processor, and the result returned. Card and bank account numbers stay with the Payment Processor and are never received by TradeRings.
11. Where a Confirmed Order is paid over a Network's payment rails on a channel other than that Network's devices, the Network whose rails carried the payment.

2.4 Communications and messaging-channel information

The Platform ingests order signals from inbound communication channels including chat (WhatsApp), email, and integrated channels. We may collect, process, and store:

1. The content of messages, including text, images (photographs of handwritten notes, product references, attachments), voice messages, and documents (PDFs, spreadsheets) supplied by your customers or by you.
2. Channel metadata, including sender identifiers (mobile number, email address), timestamps, and the inbound channel through which a message was received.
3. The interpreted intent extracted by the Automated Order Services and the structured order draft produced from it.

We collect this information solely to operate the order capture, pricing, confirmation, and handover functions of the Platform, and to keep an audit trail of how each Confirmed Order was produced from the underlying signal.

2.5 Integration and ERP-sourced information

Where an Organisation connects an ERP system or other Integrated Service to the Platform, we collect data routed through that integration, which may include:

1. Customer master data (organisation names, contact persons, addresses, payment terms, account balances).
2. Product master data (SKUs, descriptions, units of measure, tax codes, images, specification documents).
3. Pricing data (price lists, customer-specific pricing, promotions).
4. Inventory data (stock levels, available-for-sale quantities).
5. Order and order-status data flowing between the Platform and the ERP.

The direction and cadence of these data flows are configured in the integration specification agreed with the Organisation. We process integration data only to the extent necessary to provide the integration and the dependent Platform services.

2.6 Technical information

We automatically collect certain technical information when you use the Platform, including IP address, browser type and version, operating system, access times and dates, pages viewed, features used, device identifiers, and error logs. We also record:

1. Guide, documentation and video access logs, per Profile and Account: which guide or video was opened, when, and on which device.
2. Watermark traces: the Account-specific mark placed on each guide page and video frame served to you, so that a copy can be traced to the Account it was served to.
3. Rate-limit and session-control events: requests above the published limits, concurrent sessions, and the controls applied to them.

2.7 Acceptance event records

We record, against each acceptance of a TradeRings legal document on the Platform (Platform Services Agreement, Fee Schedule, User Terms of Use, Acceptable Use Policy, Market Owner Addendum, Market Member Joining Addendum, Originator Terms, and the Gate Text shown at each acceptance gate):

1. The Profile ID of the accepting individual.
2. The individual's name as registered and, where the individual is verified, as verified.
3. The IP address and the device identifier.
4. A snapshot of the Gate Text shown.
5. The name and version of each document accepted.
6. The timestamp.
7. The Organisation and the Market, where applicable.

We keep these records as the record of who accepted, on whose behalf, and what they accepted: to evidence the lawful basis for our processing and the binding effect of the documents, and, where the person who accepted is personally liable under the User Terms of Use (section 8) or the Platform Services Agreement (clause 9.4), to hold that person to it.

2.8 Originator registration

Where an Account is registered as an Originator, or enters the account number of an Originator, we collect:

1. The originator field entered at Account creation: the Originator's account number and the time it was entered; and the recruiter field entered at acceptance of the Originator Terms: the recruiting Originator's account number and the time it was entered.

2. The Originator's acceptance of the Originator Terms, its registration and status (active, in its trailing year, ended or removed), its yearly proof of existence result, its completion of the Originator Academy, the competing businesses it declared at registration (Originator Terms 8.11(2)), and the reason any originator fee ended. To prevent self-origination and self-recruitment we compare the owners and beneficial owners recorded at verification of the Accounts concerned (Originator Terms 2.4, 3A.6).
3. Originator statements: per Market and per Network, the Market, the owning Account, the confirmed order value, the platform fee received and the originator fee; and per Recruited Originator, the originator fee of each Market and Network in its window, the equal recruitment fee and the window's end date.
4. Payout data: the verified bank account in the Account's name, the bank-verification result, payout amounts, the payout provider's reference and failed payments.
5. Tax forms (for example W-8 and W-9) and the tax identification number given on them.

3. How We Collect Information

We collect information from you when you:

1. Register a Profile on the Platform.
2. Create an Account or accept an invitation to join one.
3. Complete your profile or your Organisation's profile.
4. Create or join a Market.
5. List products or configure pricing, inventory, or fees.
6. Engage in trading activity.
7. Confirm orders.
8. Communicate through the Platform.
9. Contact our support team.
10. Connect an ERP or other Integrated Service.
11. Upload documents or other Content to the Platform.
12. Accept a legal document at an acceptance gate.
13. Open a guide, documentation page or video on the Platform.
14. Verify your identity, register as an Originator, or enter an Originator's account number.

We may also collect information about you from third-party sources, including other Accounts (for example an Originator's account number entered by the Account it onboarded, or the device identity reported by a Network), public databases and registries, verification services (currently Sumsub), Payment Processors (the result of a payment), payout providers, and Integrated Services you have connected.

4. How We Use Your Information

We use the information we collect for the following purposes.

4.1 Providing and operating the Platform

1. Operating and maintaining the Platform.
2. Interpreting inbound order signals through the Automated Order Services, matching them to your catalogue, applying pricing, validating inventory and trading rules, and producing structured orders for confirmation.
3. Processing Confirmed Orders and posting them to your ERP where an integration is configured.
4. Facilitating communications between Users.
5. Authenticating Users and Organisations.
6. Personalising User experience.
7. Developing new features and services.
8. Analysing aggregated usage to improve the Platform.
9. Technical troubleshooting.
10. Attributing each Confirmed Order to the Network on whose device it was confirmed, and each Account to the Originator that onboarded it.

4.2 Business operations

1. Calculating and invoicing Platform fees, and the Network Fees, Campaign Fees and logistics fees TradeRings collects for other Accounts.
2. Initiating payments through the Payment Processor chosen and recording the result.
3. Verifying User and Organisation identity.
4. Enforcing the Platform Services Agreement, the User Terms of Use, and our policies.
5. Detecting, investigating, and preventing fraud, abuse, and security incidents.
6. Calculating originator fees, issuing originator statements, applying the conditions of the Originator Terms, and paying originator fees and remittances.
7. Measuring the effectiveness of Platform features.

4.3 Communications

1. Sending administrative and transactional notifications.
2. Providing order status updates.
3. Responding to enquiries and support requests.
4. Sending service updates and announcements.
5. Marketing our services (subject to your preferences and to applicable law).

4.4 Legal and compliance

1. Complying with legal obligations, including tax reporting on originator fees.
2. Resolving disputes.
3. Enforcing our agreements.
4. Protecting the rights, property, and safety of TradeRings, our Users, and others.
5. Protecting TradeRings' intellectual property, as a legitimate interest: detecting and evidencing copying, reverse engineering and the use of the Platform to train AI models (Acceptable Use Policy section 5), and keeping the record of the reasonable measures TradeRings takes to protect its trade secrets (acceptance records, sign-in, access logs, watermarks and session controls).

5. Automated Processing by the Automated Order Services

The Platform includes automated processing components (collectively, the "Automated Order Services": the automated services within the Platform that interpret incoming order signals, match products and customers, apply pricing, validate inventory and order rules, and put orders up for confirmation). The output of the Automated Order Services is presented to a User (the buyer, the seller, or both) for explicit confirmation. No Confirmed Order is produced without that explicit confirmation; the Automated Order Services do not unilaterally bind any Organisation to a Transaction.

Where you believe the Automated Order Services have produced an incorrect interpretation or pricing on a specific order, you may request a review by contacting support@traderings.io with the order reference. A human reviewer will examine the underlying signal and the produced output and act on legitimate corrections.

6. Disclosure of Information

We disclose your information only as described below.

6.1 Trading counterparties

To facilitate Transactions, we disclose necessary information to trading counterparties within the same Market, including the Organisation name and contact details of authorised representatives, the relevant Transaction details, and the credit and payment information needed to complete the Transaction.

6.2 Market participants

When an Organisation joins a Market, certain information is visible to other participants in that Market, as configured by the Market Owner. This may include the Organisation name and details, User names and roles, trading activity, and product listings.

6.3 Service providers

We disclose information to third-party service providers that help us operate the Platform. The categories include hosting providers, card processors for TradeRings' own fees, payout providers, verification providers, analytics providers, customer support tools, communications providers, messaging-channel providers (for example WhatsApp Business Platform and email gateways), authentication providers, and security services. We require those providers to handle your information in accordance with this Privacy Policy and applicable law, and only for the purposes for which we engage them.

6.4 Originators

An Originator sees its own originator statement: per Market and per Network, the Market, the owning Account, the confirmed order value, the platform fee received and the originator fee, so that it can check its payment. An Originator never sees another Account's order detail (the products, prices, counterparties or Users behind a Confirmed Order). The Originator holds its statement in confidence (Originator Terms section 8.5).

6.5 Integrated Services selected by the Organisation

Where you connect an Integrated Service (for example an ERP, trade finance provider, credit insurance provider, foreign exchange provider, or analytics service), we disclose the relevant Transaction and master data to that Integrated Service as required to provide the integration. You control which Integrated Services are enabled.

6.6 Aggregated and anonymised data

We may disclose aggregated and anonymised data derived from Platform usage for the purpose of improving the Platform, generating industry insights, and benchmarking. Aggregated and anonymised data does not identify any Organisation, User, customer, or Transaction.

6.7 Legal and regulatory authorities

We may disclose your information where required to do so by law or in response to a valid request from a public authority such as a court or government agency. Where lawful and practicable, we will notify the affected Organisation before disclosure.

6.8 Business transfers

If TradeRings is involved in a merger, acquisition, or sale of all or a portion of its assets, your information may be transferred as part of that transaction. We will notify you and, where required, give you a choice before your information becomes subject to a different privacy policy.

6.9 Notification of non-payment or breach

Where an Organisation fails to settle undisputed Platform fees, materially breaches the Platform Services Agreement in a manner that affects other participants in a Market, or is suspended or terminated under clause 5.5 of the Platform Services Agreement, we may notify the affected Market

Members of the fact and the reason, so they can make informed decisions about continuing to trade with that Organisation. We do not publish details of non-payment or breach on our public website or other public channels. Disclosure is limited to Market Members with a legitimate interest and is made in accordance with applicable law.

6.10 Consent

We may disclose your information to other third parties where you have provided your explicit consent.

6.11 Networks

A Network receives the data of Confirmed Orders placed through its own channel: what it needs to verify its Network Fee and statement (the Market, the order reference and value, the device and the time). For a Confirmed Order placed off its devices and paid over its payment rails, it receives only the merchant identifier, the order value and the supplier, never the order details. It receives nothing else about Markets or orders on other channels (Platform Services Agreement clause 7.2(5)).

Where the Account owner grants it on the Platform, the Network receives this data under a recorded consent. Line prices are never included. The Network may use the data for its own business, including selling it, under its own terms and privacy policy, and is responsible for that use. The Account owner may revoke the grant at any time; from then on the Network receives no new data, and the Account can no longer order through that Network but can still trade on the Platform. Data the Network already holds stays with it.

Where the Account owner grants it on the Platform, market owners on a Network receive the Account's business name, trading area and business category, and may use them only to invite the Account to their Market, never to sell or pass them on. Contact and delivery details reach a market owner only once the Account accepts an invitation and joins its Market. The grant can be revoked at any time.

We keep a record of every grant and revocation (who granted it, when, on which screen and which text version) and a log of every time a grantee reads data under it.

6.12 Logistics Providers

A Logistics Provider receives the details of Confirmed Orders (including the delivery details, the contact person for delivery, volumetric data and tariff codes) of the trading parties with which it has agreements, and only with the consent of the Market Owner concerned, given on the Platform and withdrawable there (Market Owner Addendum clause 2.15). The Logistics Provider uses those details for its own logistics services, on its own terms; TradeRings has no liability for those services.

6.13 Payment Processors

When a payment is initiated from the Platform, the Payment Processor chosen receives what it needs to initiate the payment (the order reference, the amount and currency, and the payer and payee as the Payment Processor identifies them) and returns the result to the Platform. The

Payment Processor contracts directly with the buyer and the seller and processes their payment data under its own privacy terms.

7. Verification, Credit, and Reference Checks

Where required to operate the Platform safely and lawfully, we may verify Organisation and User identity and, in future, may carry out credit and reference checks. By using the Platform, you consent to:

1. Verification of business registration, tax registration, and authorised-representative information against public registries and verification services.
2. Verification of identity documents you submit as part of any Know Your Customer process. The verification provider (currently Sumsub) collects the document and the selfie, carries out the face check, including the yearly re-check for Originators, and returns its result to TradeRings (section 2.1).
3. Where credit checks are introduced and you opt in or are notified, the receipt of credit reports from credit reporting agencies.

We use the information collected through these checks to verify your identity, assess fitness to operate on the Platform, manage risk, prevent fraud, and protect Platform integrity. Completion of any such check by TradeRings is for the Platform's internal risk management only; it is not a representation or warranty by TradeRings to any other Organisation as to identity, authority, or fitness to transact (see Platform Services Agreement clauses 3.4 and 5.3).

8. Data Security

We implement technical and organisational measures to protect information from unauthorised access, disclosure, alteration, and destruction. These include encryption of data in transit and at rest where appropriate, access controls and authentication, regular security assessments, employee training on data protection, and incident-response procedures.

No method of transmission over the internet or electronic storage is fully secure. While we use commercially reasonable measures to protect your information, we cannot guarantee absolute security. The limits of cybersecurity protection, and the corresponding allocation of risk, are set out in clause 8.3 of the Platform Services Agreement.

We will notify the affected Organisation and, where required by applicable law, the relevant supervisory authority and affected individuals, of personal data breaches within the timeframes set by that law.

9. Data Retention

We retain your information for as long as necessary to fulfil the purposes set out in this Privacy Policy, unless a longer retention period is required or permitted by law. The criteria we use to determine retention periods include:

1. The duration of our relationship with you.
2. Legal obligations to which we are subject (including tax record-keeping).
3. The duration of any limitation period applicable to potential legal claims.
4. The need for evidence of Confirmed Orders, Platform actions, and acceptance events.

On termination of an Account, Confirmed Orders and the audit trail necessary to evidence them are retained for the period required by law. Other personal information is deleted or anonymised in accordance with our retention schedule. Where the Organisation has no amounts owing at termination, an export of historical trading data may be requested under clause 10.4(6) of the Platform Services Agreement.

Acceptance event records (section 2.7), guide and video access logs and watermark traces (section 2.6) are kept for the life of the Account and for five years after it closes, the survival period of Acceptable Use Policy section 5.11 and Platform Services Agreement clause 9.4(13), and are then deleted, unless a claim or legal hold requires them to be kept longer.

10. Your Rights and Choices

Depending on your location and applicable law, you may have rights in relation to your personal information, which may include:

1. Access to your information.
2. Correction of inaccurate or incomplete information.
3. Deletion of your information, subject to legal and operational retention requirements.
4. Restriction or objection to processing.
5. Portability of your information in a structured, commonly used format.
6. Withdrawal of consent, where processing is based on consent.
7. Lodging a complaint with a supervisory authority.

To exercise any of these rights, contact privacy@traderings.io. We will respond within the period required by applicable law.

11. International Data Transfers

TradeRings operates internationally, and your information may be transferred to, stored, and processed in countries other than the one in which you reside, including the United States and any other country in which our hosting providers or service providers operate.

Where we transfer personal information out of jurisdictions with restrictions on cross-border data transfer (including the European Economic Area, the United Kingdom, and South Africa), we put in place appropriate safeguards, which may include the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, or transfer mechanisms recognised under POPIA, as relevant.

12. Children's Privacy

The Platform is intended for use by businesses and their authorised personnel. It is not intended for individuals under the age of 18, and we do not knowingly collect personal information from children. If we learn that we have collected personal information from a child, we will delete it.

13. Cookies and Similar Technologies

We use cookies and similar technologies to operate and improve the Platform. We use the following broad categories:

1. **Strictly necessary cookies.** Required for the Platform to function, including session management and security. These cookies cannot be disabled without breaking the Platform.
2. **Functional cookies.** Remember your preferences (for example language, layout) so the Platform can be tailored to you.
3. **Analytics cookies.** Help us understand how the Platform is used so we can improve it. Used in aggregate.
4. **Marketing cookies.** Used on the public website only, to measure the effectiveness of our marketing.

You may set your browser to refuse some or all cookies. Disabling strictly necessary cookies will break parts of the Platform. Where required by applicable law, we display a consent banner that lets you choose which categories to allow.

14. Third-Party Links and Services

The Platform may contain links to third-party websites and services. This Privacy Policy does not apply to that third-party content. We recommend reviewing the privacy policies of any third-party site or service before providing it with your information.

15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Updates take effect when posted, with the version and effective date at the top revised accordingly. Where a change is material, we will give prominent notice on the Platform and, where required, ask you to acknowledge the updated policy before continuing to use fee-bearing functions.

16. Contact Us

Questions about this Privacy Policy or our privacy practices may be directed to:

TradeRings Corporation Email: privacy@traderings.io Address: 55 NE 5th Ave, Suite 501, Boca Raton, FL 33432, USA.

17. Jurisdiction-Specific Provisions

17.1 South Africa (POPIA)

If you are located in South Africa, or your personal information is processed in connection with activities carried out in South Africa, the Protection of Personal Information Act, 2013 (POPIA) applies. TradeRings processes personal information in accordance with the conditions for lawful processing set out in Chapter 3 of POPIA, including accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data-subject participation.

Operator details for the purposes of POPIA: TradeRings Corporation acts as the responsible party in respect of the information described in section 2 above, except where it acts as an operator on behalf of an Organisation in relation to that Organisation's customer master data, product master data, pricing, or messaging-channel content (section 2.4 and 2.5). In those cases the Organisation remains the responsible party and TradeRings processes the data on its behalf in accordance with the Platform Services Agreement.

Acceptance records naming the individual, guide access logs and watermark traces are processed to conclude and enforce the agreements the individual accepted and to protect TradeRings' legitimate interests (section 11(1)(b) and (f)). Disclosure of order details to a Logistics Provider is made on the Market Owner's instruction and consent, as responsible party for its customers' information (section 6.12). Biometric information used in the face check is special personal information; it is processed by the verification provider with the individual's consent, and TradeRings receives only the result (section 2.1).

Data subjects in South Africa may contact the Information Regulator at inforeg@justice.gov.za with concerns that have not been resolved through privacy@traderings.io.

17.2 European Union and United Kingdom (GDPR / UK GDPR)

If you are located in the European Union or the United Kingdom, we process your personal information in accordance with the General Data Protection Regulation (EU 2016/679) or the UK GDPR, as applicable. Lawful bases on which we rely include performance of a contract (Article 6(1)(b)), our legitimate interests in operating, securing, and improving the Platform (Article 6(1)(f)), compliance with legal obligations (Article 6(1)©), and your consent where required (Article 6(1)(a)). You may exercise the rights listed in section 10 and lodge a complaint with your local supervisory authority.

Acceptance records naming the individual rest on Article 6(1)(b) and (f); guide access logs, watermark traces and rate-limit and session-control events on Article 6(1)(f), the protection of TradeRings' trade secrets; originator payout data on Article 6(1)(b), and tax forms on Article 6(1)©. The face check is biometric data under Article 9; it is processed by the verification provider on the individual's explicit consent (Article 9(2)(a)). The Automated Order Services do not take decisions based solely on automated processing that produce legal effects (Article 22): every order is confirmed by a person, and a human review is available (section 5).

17.3 California (CCPA / CPRA)

If you are a California resident, you may have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), including the right to know what personal information we collect, the right to delete personal information we have collected, the right to correct inaccurate personal information, the right to opt out of the sale or sharing of personal information, and the right to limit use of sensitive personal information. TradeRings does not sell personal information for monetary consideration.

The categories collected under this version include identifiers (name, device identifier, IP address), commercial information (Confirmed Orders, originator statements), internet or other electronic network activity (guide access logs, session-control events), and, held by the verification provider and not by TradeRings, biometric information used in the face check. Disclosures to Networks, Logistics Providers and Payment Processors (sections 6.11 to 6.13) are made to perform the services requested.

17.4 Other jurisdictions

We comply with applicable data-protection laws in the jurisdictions in which we operate. Specific supplementary provisions may apply based on your location and will be provided on request to privacy@traderings.io.

By using the Platform, you acknowledge that you have read and understood this Privacy Policy.