# TRULO CORPORATION
# PRIVACY POLICY

*Effective Date: March 1, 2026*
*Last Updated: March 1, 2026*

Trulo Corporation ("Trulo," "we," "us," or "our") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and protect your personal information when you use the Trulo Platform at jointrulo.com.

This Policy applies to all users: Hosts, Tenants, and visitors. By using the Platform, you consent to the practices described in this Policy.

## 1. Information We Collect

### 1.1 Information You Provide

Account Registration:

- Full legal name and business name
- Email address and phone number
- Password (stored encrypted — we never store plain-text passwords)
- Date of birth (for age verification)

Host-Specific Information:

- Property address, square footage, photos, and listing descriptions
- Bank account information (for payouts, processed by Stripe)
- Credit/debit card information (card on file for penalties, stored by Stripe)
- Property ownership or authorization documentation

Tenant-Specific Information:

- Business name, type, and description of intended use
- Payment method (processed and stored by Stripe — we do not store full card numbers)
- Business license or permit information (when required)

Platform Activity:

- Messages sent through the Platform between Users
- Reviews and ratings submitted
- Booking requests, confirmations, and cancellations
- Dispute submissions and communications

### 1.2 Information Collected Automatically

When you use the Platform, we automatically collect:

- IP address, browser type, and operating system
- Device identifiers and mobile carrier (for mobile app users)
- Pages visited, features used, and time spent on the Platform
- Search queries and filters used
- Referring website or application
- Approximate geographic location (city/state based on IP; we do NOT collect precise GPS coordinates)

### 1.3 Information from Third Parties

- Stripe (payment processor): Transaction data, payment success/failure status, identity verification results
- Identity verification services: Government ID scan results and liveness check data
- Insurance partners: Policy confirmation and certificate of insurance data
- Credit reporting (if applicable): Business credit information for Tenant screening

### 1.4 Information We Do NOT Collect

- Social Security Numbers
- Full credit card numbers (Stripe handles all card data)
- Precise GPS location
- Medical or health information
- Content of any communications outside the Platform

## 2. How We Use Your Information

### 2.1 To Operate the Platform

- Creating and managing your account
- Processing bookings, payments, and payouts
- Facilitating communication between Hosts and Tenants
- Generating and delivering Commercial License Agreements
- Enforcing our Terms of Service and platform policies

### 2.2 To Improve and Personalize

- Analyzing usage patterns to improve Platform features
- Personalizing search results and Listing recommendations
- Conducting internal research and analytics

### 2.3 For Safety and Security

- Verifying user identity and preventing fraud
- Investigating disputes, policy violations, and prohibited activities
- Complying with legal obligations and law enforcement requests

### 2.4 For Communications

- Sending booking confirmations, receipts, and payout notifications
- Delivering account security alerts
- Sending platform updates and policy changes (you cannot opt out of these while you have an active account)
- Sending promotional emails and product updates (you may opt out at any time)

### 2.5 For Tax and Legal Compliance

- Issuing IRS Form 1099-K to eligible Hosts
- Maintaining records required by applicable law
- Responding to subpoenas, court orders, or government requests

## 3. How We Share Your Information

### 3.1 With Other Users

When a booking is confirmed, we share limited information between Hosts and Tenants as necessary to complete the transaction: names, business names, contact information, and Space access details. We do not share full financial information between Users.

### 3.2 With Service Providers

We share information with third-party service providers who assist us in operating the Platform, including:

- Stripe, Inc. — payment processing, identity verification, and payouts
- Insurance partners — for facilitating mandatory tenant insurance requirements
- Cloud infrastructure providers — for data hosting and storage
- Email service providers — for transactional and marketing communications
- Analytics providers — for Platform usage analysis (e.g., aggregated, anonymized data)

All service providers are contractually required to handle your data in compliance with applicable law and only for the purposes of providing services to Trulo.

### 3.3 For Legal Compliance

We may disclose your information: (a) in response to a valid legal process (subpoena, court order, or government request); (b) to enforce our Terms of Service; (c) to protect the rights, property, or safety of Trulo, our Users, or the public; or (d) in connection with a merger, acquisition, or sale of all or substantially all of Trulo's assets (in which case you will be notified of the change in control).

### 3.4 What We Do NOT Do

- We do NOT sell your personal information to third-party advertisers
- We do NOT use advertising cookies or behavioral advertising networks
- We do NOT share your data with unaffiliated third parties for their own marketing purposes

## 4. Cookies and Tracking Technologies

We use the following types of cookies and similar technologies:

- Essential/Functional Cookies: Required for the Platform to operate (login sessions, booking flow, security). These cannot be disabled.

- Analytics Cookies: Used to understand how Users interact with the Platform (e.g., Google Analytics with IP anonymization). These can be disabled via our Cookie Preferences center.

We do NOT use advertising cookies, cross-site tracking, or third-party behavioral advertising. For detailed information on our cookie practices, see our Cookie Policy at jointrulo.com/cookies.

## 5. Data Retention

- Active account data: Retained for the life of your account plus seven (7) years after account closure (for legal and tax compliance)
- Transaction data (License Fees, payouts, fees): Retained for seven (7) years (IRS / tax compliance)
- Platform messages: Retained for three (3) years after the related Booking concludes
- Usage/analytics data: Retained for two (2) years in identifiable form, then aggregated/anonymized
- Identity verification data: Retained for seven (7) years (fraud prevention and legal compliance)
- Backup systems: Purged within ninety (90) days of primary deletion
- Data subject to legal hold: Retained until the legal matter is fully resolved

When the retention period expires, we delete or irreversibly anonymize your information, except where longer retention is required by law.

## 6. Your Rights and Choices

### 6.1 Access and Correction

You may access and update most of your personal information through your account settings. For information not accessible through account settings, contact privacy@jointrulo.com.

### 6.2 Deletion

You may request deletion of your account and personal information by contacting privacy@jointrulo.com. We will fulfill deletion requests subject to our retention obligations for financial records, legal holds, and fraud prevention. Deletion of your account does not delete data that Trulo is legally required to retain.

### 6.3 Data Portability

You may request a copy of your personal data in a machine-readable format (CSV or JSON) by emailing privacy@jointrulo.com. We will fulfill portability requests within thirty (30) days.

### 6.4 Opt-Out of Marketing

- Email: Click "Unsubscribe" in any marketing email or contact privacy@jointrulo.com
- Analytics cookies: Use our Cookie Preferences center at jointrulo.com/cookies

You cannot opt out of transactional emails (booking confirmations, payment receipts, legal notices) while your account is active.

### 6.5 California Residents — CCPA Rights

California residents have additional rights under the California Consumer Privacy Act (CCPA):

- Right to Know: You may request disclosure of the categories and specific pieces of personal information we have collected about you, and the purposes for which we use it.
- Right to Delete: You may request deletion of personal information subject to certain exceptions.
- Right to Opt-Out of Sale: We do not sell personal information. No opt-out is necessary.
- Right to Non-Discrimination: We will not discriminate against you for exercising your CCPA rights.

To exercise your CCPA rights, contact: privacy@jointrulo.com or [toll-free phone number].

### 6.6 EU/EEA Residents — GDPR Rights

If you are located in the European Economic Area, you have additional rights under the General Data Protection Regulation (GDPR), including the right to restrict processing, the right to object, and the right to lodge a complaint with your supervisory authority. Our legal basis for processing includes: contract performance (fulfilling your bookings), legitimate interests (fraud prevention, platform improvement), and legal obligation (tax and financial record-keeping).

### 6.7 Massachusetts Residents — M.G.L. c. 214 § 1B

Massachusetts residents have a statutory right of privacy under M.G.L. c. 214 § 1B, which protects against unreasonable, substantial, or serious interference with their privacy. Trulo's data collection and processing practices are designed to avoid unreasonable intrusion into users' private affairs. Massachusetts residents who believe Trulo has engaged in an unreasonable, substantial, or serious invasion of their privacy may:

- Contact Trulo's Privacy Officer at privacy@jointrulo.com to request a review of the alleged intrusion
- File a complaint with the Massachusetts Attorney General's Office
- Pursue civil remedies under M.G.L. c. 214 § 1B in Superior Court

Trulo commits to not collecting personal information beyond what is reasonably necessary for Platform operations, not sharing personal information in ways that would constitute a serious interference with user privacy, and providing meaningful privacy controls described in Sections 6.1–6.6.

### 6.8 Response Timeline

We will acknowledge privacy requests within five (5) business days and fulfill them within thirty (30) days. If we need additional time (up to 60 days for complex requests), we will notify you.

## 7. Data Security

We implement industry-standard security measures to protect your information, including:

- TLS encryption for all data transmitted between your device and our servers
- Encryption of sensitive data at rest
- Access controls limiting employee access to personal information to those with a legitimate business need
- Regular security audits and penetration testing
- Incident response procedures for data security events

No security system is impenetrable. In the event of a security breach or unauthorized acquisition of personal information:

### 7.1 Massachusetts Data Breach Notification — M.G.L. c. 93H

Trulo's data breach notification obligations are governed by the Massachusetts Data Breach Notification Act (M.G.L. c. 93H). In the event of a breach of security resulting in unauthorized acquisition or use of a Massachusetts resident's personal information, Trulo will:

- Notify affected Massachusetts residents as soon as reasonably possible following discovery of the breach, without unreasonable delay
- Notify the Massachusetts Attorney General's Office and the Office of Consumer Affairs and Business Regulation (OCABR) as soon as reasonably possible following discovery
- Notify consumer reporting agencies (if more than 1,000 Massachusetts residents are affected simultaneously), as required by M.G.L. c. 93H §3
- Provide notice in clear, plain language describing: the nature of the breach, the types of personal information affected, steps taken to restore security, and steps affected individuals can take to protect themselves

'Personal information' under M.G.L. c. 93H includes a Massachusetts resident's first name and last name or first initial and last name combined with any one of the following unencrypted data elements: Social Security number; driver's license or state ID number; financial account number, credit or debit card number (with or without security code); or passport number.

### 7.2 Data Disposal — M.G.L. c. 93I

When personal information is no longer needed for business purposes and Trulo's retention obligations have expired, Trulo will destroy or arrange for the destruction of such records in a secure manner that prevents unauthorized access to or use of the personal information. Secure destruction methods include secure erasure (meeting NIST 800-88 standards or equivalent), physical destruction of storage media, or cryptographic erasure of encrypted data. Trulo's data disposal obligations apply to both Trulo's own records and records held by Trulo's service providers on Trulo's behalf. This practice complies with M.G.L. c. 93I. Service providers handling Trulo data are contractually required to implement equivalent disposal standards.

### 7.3 Written Information Security Program — 201 CMR 17.00

Trulo maintains a Written Information Security Program ('WISP') as required by the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00). The WISP establishes administrative, technical, and physical safeguards designed to: (a) ensure the security and confidentiality of personal information; (b) protect against anticipated threats or hazards to the security or integrity of personal information; and (c) protect against unauthorized access to or use of personal information in a manner that creates a substantial risk of identity theft or fraud.

Trulo's WISP includes, at minimum, the following components required by 201 CMR 17.03:

- Designation of an employee or employees to maintain the WISP and coordinate security functions;
- Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper or other records containing personal information;
- Employee security awareness training on the proper use of computer security systems and the importance of personal information security;
- Means for detecting and preventing security system failures, including by monitoring and regular testing of security procedures;
- Policies and procedures addressing the proper storage, access, and transportation of records containing personal information outside of business premises;
- Disciplinary measures for violations of the WISP rules;
- Prevention of terminated employees from accessing records containing personal information;
- Reasonable restrictions upon physical access to records containing personal information;
- Regular monitoring of the program's effectiveness and upgrading of safeguards as necessary based on changed circumstances.

Trulo's technical security measures include encryption of personal information transmitted over public networks and stored on laptops or portable devices, firewall protection, up-to-date malware and antivirus software, secure user authentication protocols including multi-factor authentication for access to systems containing personal information, and encryption of personal information stored on all user devices.

The WISP is a living document reviewed and updated at least annually and whenever there is a material change to Trulo's business practices affecting personal information security. The complete WISP is maintained as an internal document and is made available to the Massachusetts Attorney General's Office upon request.

## 8. Children's Privacy

The Trulo Platform is intended for use by adults and registered businesses only. Trulo does not knowingly collect, use, or disclose personal information from individuals under thirteen (13) years of age, in compliance with the Children's Online Privacy Protection Act (COPPA, 15 U.S.C. §§ 6501–6506). The Platform is not directed to children under 13.

If Trulo becomes aware that a user under the age of 13 has created a Platform account or submitted personal information, Trulo will: (a) immediately terminate the account; (b) delete all associated personal information from Trulo's records; (c) notify the account's associated email address of the deletion; and (d) take reasonable steps to prevent re-registration.

Users between the ages of 13 and 17 may not use the Platform without an adult or authorized business entity sponsoring their account. By registering, you represent that you are 18 or older or are a duly authorized representative of a business entity.

If you are a parent or guardian who believes your child under 13 has provided personal information to Trulo, please contact privacy@jointrulo.com immediately. We will promptly investigate and, upon verification, delete all such information and notify you of the deletion.

## 9. Payment Data Security and PCI DSS Compliance

Trulo does not directly process, store, or transmit credit card numbers, bank account numbers, or other sensitive payment card data. All payment processing is performed by Stripe, Inc. ('Stripe'), a PCI DSS Level 1 certified payment service provider — the highest level of certification under the Payment Card Industry Data Security Standard (PCI DSS). Stripe's PCI DSS compliance can be verified at stripe.com/docs/security.

When you provide payment information on the Trulo Platform:

- Your card or bank account data is transmitted directly to Stripe using TLS 1.2+ encryption and is never transmitted through Trulo's servers in unencrypted form;
- Trulo receives only a tokenized representation of your payment method (a 'Stripe token') and the last four digits of your card number — not your full card number, CVV, or expiration date;
- Stripe's systems are responsible for maintaining PCI DSS compliance for all stored cardholder data. Trulo's own systems are scoped out of PCI DSS compliance requirements because Trulo does not store, process, or transmit cardholder data.

Payout processing for Hosts is also performed through Stripe Connect. Trulo may collect Host bank account information for the purpose of transmitting it securely to Stripe; Trulo does not store full bank account numbers after transmission and does not have ongoing access to Host banking credentials.

### 9.1 Fraud Detection and Payment Security

Trulo uses automated tools, including Stripe Radar and Trulo's internal risk scoring systems, to detect and prevent fraudulent transactions. These systems may analyze patterns in account activity, device information, payment behavior, and geolocation data to identify potential fraud. If a transaction is flagged, Trulo may: (a) temporarily pause a payout or booking; (b) request identity verification; or (c) reverse or void the transaction. Trulo's fraud detection is not infallible and does not constitute a guarantee against payment fraud.

## 10. Automated Processing, Profiling, and AI-Assisted Decisions

Trulo uses automated processing and algorithmic systems in several areas of the Platform. This section explains how these systems work and what rights you may have.

### 10.1 Search and Matching Algorithms

Trulo's search and Space recommendation features use automated ranking algorithms to determine which Listings are displayed to Tenants and in what order. The ranking algorithm considers factors including: listing completeness and accuracy, proximity to search location, price competitiveness, Host response rate and review score, Booking history and Platform engagement, and space characteristics matching the Tenant's stated preferences. Trulo's ranking algorithm is designed to be commercially neutral and does not intentionally discriminate based on protected characteristics. Trulo audits its search ranking algorithm annually for disparate impact.

### 10.2 Risk Scoring and Account Review

Trulo uses automated risk scoring to evaluate Tenant Booking Requests, detect unusual account activity, and determine eligibility for certain Platform features. These automated systems may analyze account history, payment behavior, booking patterns, and third-party data. Automated risk scores influence, but do not solely determine, account decisions. A human reviewer is involved in all account suspension or permanent termination decisions.

### 10.3 Automated Review Moderation

Trulo uses natural language processing (NLP) tools to automatically screen user-submitted reviews for prohibited content (profanity, personally identifiable information, discriminatory language, and commercial solicitation) before publication. Flagged reviews are routed for human review within 48 hours. Automated flagging may result in temporary delay of review publication but does not constitute a final decision to suppress a review.

### 10.4 Your Rights Regarding Automated Decisions

If you are an EU/EEA resident, you have rights under GDPR Article 22 regarding decisions made solely by automated means that significantly affect you. You may request that Trulo provide human review of any automated decision affecting your account, including risk-based declines, account restrictions, or listing suppression. To request human review, contact privacy@jointrulo.com with the subject line 'Human Review Request' and a description of the decision you wish to contest. Trulo will respond within 30 days. This right does not apply to decisions that are necessary for contract performance or are authorized by applicable law.

California residents may also exercise rights regarding automated profiling under the California Privacy Rights Act (CPRA) as described in Section 6.5 above. Massachusetts residents may exercise rights under M.G.L. c. 214 § 1B as described in Section 6.7 above.

## 11. Global Privacy Control (GPC) and Browser Privacy Signals

Trulo recognizes and responds to the Global Privacy Control (GPC) browser signal as a valid opt-out of the sale and sharing of personal information under the California Privacy Rights Act (CPRA) for California residents. The GPC is a browser or browser extension setting that communicates a user's privacy preferences to websites.

### 11.1 How Trulo Processes GPC Signals

If Trulo detects a valid GPC signal from a California resident's browser:

- Trulo will treat the signal as a request to opt out of the sale and sharing of that user's personal information for cross-context behavioral advertising purposes;
- Trulo will not sell or share personal information collected during that session for targeted advertising purposes, even if the user has not separately submitted an opt-out request;
- The GPC opt-out is processed automatically and does not require the user to submit a separate form or request.

### 11.2 Scope of GPC Opt-Out

Responding to a GPC signal does not affect: (a) Trulo's use of personal information for service delivery, billing, legal compliance, or fraud prevention; (b) the use of strictly necessary cookies required for Platform functionality; or (c) Trulo's sharing of data with service providers (such as Stripe, AWS, and Sendgrid) acting under data processing agreements where such sharing does not constitute a 'sale' or 'sharing' under applicable privacy law. Users who wish to exercise additional privacy rights beyond the GPC opt-out — such as access, deletion, or correction — must submit a separate request to privacy@jointrulo.com.

Note: GPC recognition is provided as a service to California residents. Users in other jurisdictions may use the GPC signal, but Trulo's obligation to honor it is governed by California law. Trulo will monitor applicable laws in other U.S. states and update this section as additional states adopt GPC recognition requirements.

## 12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated to registered Users via email at least fourteen (14) days before taking effect. Your continued use of the Platform after the effective date of any update constitutes acceptance of the updated Policy.

## 13. Contact Us

**Privacy Officer — Trulo Corporation**

123 Main Street, Boston, Massachusetts 02101

Email: privacy@jointrulo.com

Website: jointrulo.com/privacy