

Privacy Policy

How Rent Anything collects, uses, discloses, retains, and protects personal information

EFFECTIVE DATE	10/02/2026
LAST UPDATED	10/02/2026
VERSION	1.2
COMPANY	Rent Anything LLC d/b/a Rent Anything
PRIVACY CONTACT	martin@rentanything.org

This Privacy Policy applies to the Rent Anything mobile applications, website, marketplace, account, listing, booking, payment, notification, support, dispute, identity-verification, and related services (collectively, the "Service").

1. Information We Collect

1.1 Account and contact information

- First name, optional middle name, last name, date of birth, email address, phone number, street address, city, state, and account identifiers.
- Account status, email-verification status, acceptance records for required legal documents, login preferences, optional authentication-text consent status, consented phone number, consent source, opt-out timestamp, and security events.
- Passwords are handled through Supabase authentication and are not intended to be stored by Rent Anything in readable form.

1.2 Identity-verification information

- Images of the front and back of a government identification document submitted through guided camera capture or file upload.
- Identification expiration date, upload and review timestamps, verification status, and Support review notes.
- Information needed to determine age eligibility and whether an identification document appears current and valid.
- Rent Anything does not use the barcode data for unrelated marketing or advertising.

1.3 Listings, catalog requests, and public profile information

- Listing title, category, product, brand, model, condition, description, hourly, daily, weekly, and monthly rates, deposit, replacement value, availability, photos, city, and state.

- Product request category, product name, notes, one to four photos, ticket number, decision, and Support reason.
- Public profile information includes your name, optional profile photo, average star rating, review count, and eligible written rental reviews. Your profile photo is optional and may be added, replaced, or removed in your profile. Photo files use public delivery URLs, so someone who obtains a URL may view or copy the photo outside the app. Do not upload identification documents or other sensitive information as a profile photo.
- The Owner's exact pickup address and instructions are not part of the public listing record shown to marketplace users.
- Public profiles do not display your private email, phone number, date of birth, government identification, payment credentials, or account address. Approved handoff-address disclosure is separate, as described in Section 3.
- After a completed rental, each participant may submit one review of the other participant with a rating from 1 to 5 stars and an optional written comment. The profile displays the average of retained ratings and a review count; ratings from both renter and owner roles contribute to that average. Review text, rating, date, and reviewer name may be visible to eligible marketplace users. A rating is a user's opinion, not a safety guarantee or certification.

1.4 Bookings, handoffs, and transaction records

- Requested dates and times, pricing unit, rental subtotal, service fees, deposit, status, invoice number, cancellation or decline activity, and participant identifiers.
- Pickup and drop-off code status, code-attempt security data, pickup time, return-submission time, Owner review deadline, completion time, and settlement results.
- Exact handoff address and instructions after booking acceptance and during the active pickup or return workflow.
- Disputes, messages, support questions, evidence, photos, receipts, repair or replacement information, and resolution records.
- Booking-message content, sender and recipient identifiers, booking association, sent and read timestamps, delivery records, and authorized Support access logs. Booking messages are available only to the Owner and Renter after acceptance, while the booking is in an eligible accepted, pickup, active-rental, return-review, or disputed status. There is no open messaging directory. Participant access closes when the booking is completed, cancelled, or declined. Messages remain in protected transaction records for authorized Support review under the Privacy Policy; ending participant access does not immediately delete them.

1.5 Payments and payouts

- Payment status, Stripe customer or connected-account identifiers, PaymentIntent identifiers, charge and refund identifiers, transfer and payout status, and limited payment-method details such as brand or last four digits.
- Stripe handles complete payment-card and bank-account credentials. Rent Anything stores limited payment references and status information, not complete card numbers or bank login credentials. Device biometric templates remain with the operating system; Stripe Identity may process identification and selfie data separately for identity verification.
- Owner earnings, available payout balance, weekly payout records, Instant Payout requests, and applicable 1.25% Instant Payout fee.

1.6 Location, address search, and navigation

- City and state entered by a user and approximate coordinates used for nationwide and distance-based product search.
- Device location only when the user chooses a location-based feature and grants foreground permission.
- Address text and suggestion selections processed through Google Places or mapping services to autocomplete an address.
- Navigation destination data when a user opens the in-app map or the phone's navigation application.

1.7 Device, notification, and technical information

- Expo push token, device platform, notification preferences, app version, and delivery status needed to send transactional app notifications, plus limited authentication-text consent and delivery records.
- Device-local settings for Keep Me Signed In and biometric unlock. Face ID, fingerprint, or device-passcode templates are managed by the operating system and are not provided to Rent Anything.
- Internet Protocol address, request timestamps, error reports, security logs, fraud signals, and similar technical records generated by the Service or its providers.

2. How We Use Information

- Create, verify, secure, and administer accounts and enforce the 18-and-older requirement.
- Review identification, remind users before identification expiration, and restrict access when re-verification is required.
- Display and search approved listings, process product requests, and prevent users from renting their own products.
- Create and administer bookings, calculate pricing and fees, stage handoff codes, show navigation, and document pickup and return.
- Process rental charges, separate deposit charges and refunds, Owner transfers, weekly payouts, and eligible Instant Payouts through Stripe.
- Send email, push, payment, return, identity, safety, support, and policy communications, and send optional one-time authentication texts when a user has affirmatively consented.
- Resolve disputes, prevent fraud, enforce prohibited-item and conduct rules, protect users and property, and comply with law.
- Debug, maintain, measure, and improve Service reliability, accessibility, security, and user experience.

3. Exact Address and Handoff Privacy

Public search and product cards use city, state, and approximate location information. An exact pickup or drop-off address is disclosed only through restricted booking functions to the Owner and the accepted Renter when needed for the handoff.

After the Renter enters the correct drop-off code and submits the return, the booking's exact handoff address and instructions are removed from participant access and are not displayed in completed history or invoices. The Owner's underlying private listing address may remain stored

so the Owner can make that product available again, unless the Owner changes or deletes the listing. Limited copies may persist temporarily in protected backups, security logs, or legal records.

4. How We Disclose Information

4.1 Other marketplace users

We disclose listing information, public profile details, city and state, booking status, and transaction information to the other participant as needed. Exact handoff information is restricted as described above. Owner-only financial information and Support-only records are not disclosed to standard users.

4.2 Service providers

- Supabase for authentication, database, storage, server functions, and security controls.
- Stripe for renter payments, deposits, refunds, connected payout accounts, transfers, payouts, and Stripe Identity document and selfie verification. Stripe may compare a submitted selfie with identification information and provide verification results; its own legal and privacy notices also apply.
- Resend for account, transaction, support, and policy email.
- Expo, Apple Push Notification service, and Firebase Cloud Messaging for app delivery and push notifications.
- Google Maps and Google Places for address suggestions, map display, geocoding, distance search, and navigation.
- Apple and Google for app distribution, device services, and operating-system security.
- Twilio is the planned provider for optional one-time authentication texts if that feature is enabled after the required provider approvals and affirmative user consent. It is not an active rental-notification or marketing-text provider in the initial store release.

4.3 Legal, safety, and business disclosures

We may disclose information when reasonably necessary to comply with law or legal process; respond to lawful government or law-enforcement requests; protect users, property, or the Service; investigate fraud, theft, threats, injury, prohibited items, or abuse; enforce agreements; obtain professional advice; or complete a merger, financing, acquisition, reorganization, or sale subject to appropriate safeguards.

5. No Sale or Behavioral Advertising

Rent Anything does not currently sell personal information for money or use it for third-party cross-context behavioral advertising. We do not share mobile phone numbers, authentication-text consent records, or other mobile information with third parties or affiliates for marketing or promotional purposes. We may disclose mobile information to service providers, such as Twilio, solely as necessary to deliver and administer user-requested authentication texts. If our sale or advertising practices change, we will update this Policy and provide choices required by applicable law before the change applies.

6. Identification Review and Expiration

Identification submissions are stored in a restricted private area and may be accessed only by authorized Support personnel and identity-verification service providers that need the information for verification, fraud prevention, safety, or legal compliance. We disclose identification information to a government authority only when permitted or required by law. A standard user may not enter the marketplace until required identity review is approved.

We may send a reminder approximately 30 days before the submitted identification expires. Marketplace access may be temporarily suspended on or after expiration until updated identification is submitted and approved. Rejected submissions may include a Support explanation. Identification images, verification records, and any biometric data are retained and deleted under Section 8.

7. Notifications and Communications

We send essential account and transaction communications by email and may send push notifications after permission is granted. A current phone number is required for account and safety records, but authentication text messages are optional. During registration, a user may check the separate, unchecked authentication-text consent box and choose Continue With Texts, or choose Opt Out. A user may also enable or disable Authentication Texts in Login Security. Accepting a legal document, providing a phone number, or creating an account does not by itself provide text-message consent.

Authentication texts are not active in the initial store release; account verification and password reset use email. If this optional feature is enabled later, separate affirmative consent will be required before any authentication text is sent, and email will remain available.

Optional text messages are limited to one-time account verification and password reset codes. Message frequency varies based on user-requested verification and password-reset activity. Message and data rates may apply. Reply STOP to opt out or HELP for help. Email remains available when texts are declined or unavailable. Rent Anything does not send rental or marketing text messages through this program. Changing the saved phone number disables the preference until the user separately consents for the new number.

8. Retention

8.1 General retention rule

Rent Anything retains personal information only for as long as reasonably necessary and proportionate to provide the Service and for the purposes described in this Policy. We may retain information longer when needed to comply with law, maintain tax or accounting records, resolve a dispute or chargeback, enforce an agreement, prevent fraud, protect safety, or establish, exercise, or defend legal claims. When information is no longer needed, we delete it, de-identify it, or make it inaccessible, subject to backup rotation and a documented legal hold.

8.2 Identification-verification schedule

- Incomplete registration. If account verification is not completed during the seven-day verification period, submitted identification images and associated pending-verification data are scheduled for deletion or de-identification within 30 days after that period expires.
- Approved or rejected submission. We delete the front and back identification images within 90 days after the final verification or review decision. Any biometric identifier or biometric template created for identity matching is deleted or redacted within 30 days after the verification purpose is complete, unless a shorter period applies.
- Replacement identification. When a user replaces an expired or superseded identification document, we delete the prior images within 30 days after the replacement review is final.
- Verification record. We retain a limited record of the verification result, document type, expiration date, submission and review timestamps, reviewer action, and necessary fraud or safety flags while the account is active and for three years after account closure. This limited record does not include the raw identification images or a biometric template.
- Extended hold. If a submission is reasonably necessary for an open fraud investigation, identity appeal, dispute, security incident, subpoena, court order, or other legal obligation, we retain only the information needed for that matter and delete it within 30 days after the hold ends, subject to any shorter state-law limit.
- Device biometrics. Face ID, fingerprint, and device-passcode templates remain with the device operating system. Rent Anything does not receive or retain those templates.

8.3 Account, marketplace, and transaction schedule

- Account and profile data. We retain account and profile information while the account is active and for three years after account closure, except that data subject to a valid deletion request is deleted sooner unless an exception applies.
- Profile photos. Removing or replacing a photo removes its active profile association and requests deletion of the former stored object. Cached or backup copies may persist as described below, and copies already obtained by other people are outside our control.
- Booking messages and reviews. Booking conversations, associated Support access records, and transaction-linked reviews follow the seven-year booking and dispute retention schedule, unless earlier deletion, de-identification, or a documented legal hold applies. Completed-booking messages are not available in participant history but remain accessible to authorized Support for safety, fraud, disputes, and legal needs. Retention of a record does not mean that it remains publicly displayed.
- Listings and product requests. Public listing content remains until the Owner edits or removes it, the account is deleted, or Rent Anything removes it. Product-request records and non-transaction Support requests are retained for three years after the request is closed. Transaction-linked content follows the booking schedule below.
- Bookings and financial records. Booking, invoice, payment, deposit, refund, payout, tax, dispute, chargeback, and settlement records are retained for seven years after the transaction is completed or the matter is finally resolved. Complete card and bank-account credentials remain with Stripe and are not retained by Rent Anything.
- Handoff addresses. The booking copy of the exact pickup or drop-off address and instructions is removed from participant access and the completed booking workflow after return submission and is not displayed in history or invoices. The Owner's private listing

address remains while needed to operate that listing. Residual backup copies are overwritten on the schedule described below.

- Device, notification, and authentication-text data. Push tokens and device preferences are retained until replaced, disabled, invalidated, or no longer needed. Authentication-text consent remains active only for the consented phone number until withdrawn; limited consent, opt-out, challenge, and delivery records are retained under the account schedule or for up to 12 months when maintained as security logs, unless a longer period is needed for an investigation or legal obligation.

8.4 Backups and legal holds

Deleted information may remain in encrypted or access-restricted backups until those backups are overwritten in the ordinary course, generally within 90 days. Backup data is not restored to active use except for disaster recovery, security, or legal compliance. A documented legal hold pauses deletion only for the specific information and period reasonably necessary for the matter.

8.5 State-specific retention rules

The following provisions apply when the cited law covers Rent Anything and the information at issue. An ordinary photograph is not treated as a biometric identifier where a state law excludes photographs; the biometric rules apply if Rent Anything or a verification provider creates, controls, or processes data that meets the applicable statutory definition. If another applicable law requires an earlier deletion date, the earlier date controls.

California

For California personal information and sensitive personal information, we apply the category-specific periods in this Section and do not retain information longer than reasonably necessary and proportionate for each disclosed purpose. If a fixed period cannot reasonably be stated, we use the criteria in Section 8.1. (Cal. Civ. Code Section 1798.100(a)(3) and (c).)

Colorado

If we control or process a Colorado biometric identifier, we delete it by the earliest of: the date the initial collection purpose is satisfied; 24 months after the consumer's last interaction with us; or no more than 45 days after an annual review determines that storage is no longer necessary, adequate, or relevant. A single additional period of up to 45 days may be used only when the statute permits it. We review retained biometric identifiers, photographs used for identification, and related data at least annually. (Colo. Rev. Stat. Section 6-1-1314; 4 CCR 904-3, Rule 6.07.)

Illinois

If we possess an Illinois biometric identifier or biometric information, we permanently destroy it when the initial purpose for collection has been satisfied or within three years after the individual's last interaction with Rent Anything, whichever occurs first, unless a valid warrant or subpoena requires otherwise. This Section serves as the public retention schedule and destruction guideline for that information. (740 ILCS 14/15(a).)

Minnesota

For personal data covered by the Minnesota Consumer Data Privacy Act, we do not retain data that is no longer relevant and reasonably necessary for the disclosed collection and processing

purposes, unless retention is otherwise required by law or permitted by that Act. (Minn. Stat. Section 325M.16, subdivision 2(g).)

Texas

If we possess a Texas biometric identifier captured for a commercial purpose, we destroy it within a reasonable time and no later than one year after the collection purpose expires. If another law requires an associated instrument or document to be kept longer, we destroy the biometric identifier within a reasonable time and no later than one year after that legal retention requirement ends. (Tex. Bus. & Com. Code Section 503.001(c)(3) and (c-1).)

Washington

If we knowingly possess a Washington biometric identifier enrolled for a commercial purpose, we retain it no longer than reasonably necessary to provide the enrolled service, protect against fraud, criminal activity, claims, security threats, or liability, or comply with a court order or applicable law. (RCW 19.375.020(4)(b).)

8.6 Retention review

We review this schedule and the data covered by it at least annually and after a material change to the Service, identity-verification process, provider, or applicable law. We direct service providers to delete or return data at the end of their services unless continued retention is legally required.

9. Account Deletion

Users may request deletion in Profile > Account > Account Management or at <https://rentanything.org/account-deletion>. Deletion is blocked while a rental, return, dispute, deposit, or payout is active or unsettled. A three-business-day safety hold begins after the final rental is fully settled.

After deletion, profile data and active marketplace content are deleted or de-identified, subject to retention described above. A confirmation email is sent when deletion completes. The designated Support account cannot be deleted through the standard in-app workflow.

10. Your Choices and Privacy Rights

- Review and correct personal information through Personal Information and Identification settings.
- Manage biometric unlock, Keep Me Signed In, push permissions, and optional Authentication Texts through app or device settings. Authentication texts may also be stopped by replying STOP.
- Request access, correction, deletion, or a copy of personal information by contacting Support.
- Appeal a denied privacy request where applicable by replying to the decision and writing "Privacy Appeal" in the subject line.
- Use an authorized agent where applicable, subject to verification of the request and the agent's authority.
- We do not discriminate against users for exercising privacy rights, although deleting or withholding information required for the Service may prevent use of affected features.

11. Security

We use role-based access, Row-Level Security, private storage, server-side authorization, authentication, encryption in transit, staged handoff secrets, restricted Support tools, and other administrative, technical, and organizational measures. No system is completely secure. Users must protect credentials, devices, codes, and payment methods and report suspected unauthorized access promptly.

12. Children

The Service is limited to persons age 18 or older and is not directed to children. We do not knowingly permit a person under 18 to create an account. Contact us if you believe a minor provided personal information.

13. State-Specific Rights

Depending on residency and applicable law, users may have rights to know, access, correct, delete, or obtain a portable copy of personal information; limit or withdraw consent to certain processing; and appeal a denied request. A request may be submitted through in-app Support or by emailing martin@rentanything.org with "Privacy Request" in the subject line. We may verify the requester's identity and an authorized agent's authority before acting. We do not discriminate against a user for exercising a privacy right, although some information is necessary to provide the Service.

14. Changes to This Policy

We may update this Privacy Policy prospectively. Material changes may be communicated by email, in-app notice, push notification, or another reasonable method. The updated Policy will identify its effective date.

15. Contact

Rent Anything LLC d/b/a Rent Anything

Privacy and Support Email: martin@rentanything.org

Website: <https://rentanything.org>

Electronic acknowledgement

BY CHECKING THE PRIVACY POLICY BOX, I ACKNOWLEDGE THAT I HAVE READ THIS PRIVACY POLICY AND UNDERSTAND HOW RENT ANYTHING HANDLES INFORMATION.