PRIVACY POLICY

StarProve — IVirgo LLC

Last Updated: May 8, 2026

IVirgo LLC ("we," "us," or "our") operates the StarProve mobile application available on the Apple App Store (the "App"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our App.

The App is a community tool designed for verified contractors to share their direct, firsthand experiences with clients at specific job sites.

Please read this Privacy Policy carefully. By accessing or using the App, you signify that you have read, understood, and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Policy and our Terms and Conditions.

1. INFORMATION WE COLLECT

StarProve requires full KYC verification for all access. There is no anonymous, guest, or partial access of any kind. Access is granted only upon successful completion of KYC verification.

IVirgo LLC collects the absolute minimum data necessary to operate the platform.

IVirgo LLC does NOT store: personal documents, license numbers, business records, or identity documents. KYC documents are reviewed by IVirgo LLC's internal verification system, held temporarily in an encrypted S3 bucket, and permanently deleted (hard delete) immediately after the verification decision. IVirgo LLC receives only a verified/not verified signal.

IVirgo LLC does not store Google or Apple authentication credentials.

1.1 Account Creation

Account Information

When you create an account, we collect:

- Via Google Sign-In: your name and email address as provided by Google via OAuth 2.0. We receive only what you approve during sign-in. We do not receive your Google password or access to other Google data. Google's privacy policy applies: policies.google.com/privacy
- Via Apple Sign-In: your name and email address (or Apple's anonymized relay email if you choose to hide your email). We do not receive your Apple ID password or access to other Apple data. Apple's privacy policy applies: apple.com/privacy
- Via email registration: your name and email address as entered by you

1.2 KYC-Verified Contractors

All users must complete KYC verification before accessing any part of the platform. Upon successful verification, users receive full platform access.

Account and Profile Information

KYC-verified members provide the following during registration:

- Work Category (Trade Type): your professional trade or service category self-selected during KYC registration (e.g., Painting, Electrical, Plumbing, HVAC, General Contractor). Used solely to verify your professional license during the KYC process. Not displayed to other users and not included in your anonymous Contractor ID.

- Contractor ID: an anonymous alphanumeric identifier (e.g., Verified · #SP-6CF27B3F) automatically assigned upon successful KYC verification. This ID is the only author identifier displayed on Professional Experiences. Business name, company name, personal name, and work category are never shown to other users.
- KYC verification: Documents are encrypted in transit (HTTPS/TLS), stored temporarily in IVirgo LLC's private S3 bucket (kyc-private/), reviewed manually by an authorized administrator, and permanently deleted (hard delete) immediately after the verification decision. No documents are retained after deletion.
- Years of experience (optional, for internal platform improvement only)
- Service areas (optional, for internal analytics only)
- Professional documentation submitted to IVirgo LLC internal verification system (contractor license, business license, insurance certificate, or trade certification) — reviewed and then permanently deleted; not retained by IVirgo LLC

Professional Experiences

When a Verified Contractor submits an Experience, we collect:

- The Job Site address
- Color-coded assessment (green, yellow, or red)
- Three job site condition indicators: payment conditions at the site, work environment, likelihood of returning to the address
- Optional text description
- Assigned Contractor ID: your anonymous numeric ID (#XXXX) is associated with your Experience for moderation purposes. This ID (not your business name) is what other users see.

Communications

Information you provide when contacting us for support or sending feedback.

1.3 Information Collected Automatically (Verified Members Only)

The following is collected automatically for all KYC-verified users for security, performance, and app improvement:

Usage Data

- Features you use and time spent on the App
- Map interactions within the 10-mile local radius display
- Actions taken within the App

Device Information

- IP address
- Device type and model
- Operating system and version
- Unique device identifiers (for security and fraud prevention only)

Location Data

The App uses addresses entered by contractors to display job site locations on a map. We do not collect your device's precise GPS location unless you explicitly grant permission for map navigation features.

- Job site addresses entered by contractors are stored as location identifiers
- We do not share your device's GPS coordinates with third parties
- You may disable location permissions in your iOS Settings at any time

1.4 App Tracking Transparency (iOS)

In compliance with Apple's App Tracking Transparency (ATT) framework:

- We do not track you across third-party apps or websites for advertising purposes.
- We do not use the Identifier for Advertisers (IDFA)
- No ad networks, no IDFA, no behavioral tracking

If we add tracking features in the future, we will update this policy and request your explicit permission through the iOS ATT prompt before any tracking begins.

2. HOW WE USE YOUR INFORMATION

We use the information we collect for the following purposes:

- To Provide and Maintain the App: Including verifying your contractor status and allowing you to view and share experiences based on job site addresses.
- To Facilitate Community Sharing: To display your experiences and ratings to other verified contractors, helping them make informed decisions before starting a job.
- To Present Aggregated Subjective Assessments: We use the color-coded assessments you provide (based on job site conditions: payment conditions, work environment, and likelihood of return) to calculate and display an Aggregate Site Signal (red, yellow, or green) for each job site address. This signal represents the aggregated professional opinions of Verified Contractors about working conditions at that address and is presented for informational purposes only. The colors do not constitute a determination by StarProve about any specific client.
- To Verify Contractor Identity: We transmit the professional documentation you submit to our internal verification system for automated and/or manual review. The system confirms whether your documents are valid and authentic and returns a verification result to us. We do not independently store copies of your identity documents — documents are temporarily stored on IVirgo LLC servers and permanently deleted after review.
- To Improve Our App: To understand how our service is used and to develop new features.
- To Communicate With You: To send you updates, security alerts, and support messages.
- To Ensure Compliance and Safety: To detect, prevent, and address fraud, unauthorized use, and violations of our Terms and Conditions.

3. SHARING YOUR INFORMATION

We do not sell, trade, or rent your personal information to third parties for marketing purposes. We may share information in the following limited circumstances:

3.1 Visibility on the Platform

All content on StarProve is visible only to KYC-Verified Contractors. There is no partial or limited access tier.

Visible to all KYC-Verified Contractors:

- Aggregate Site Signal color: the single anonymous color (green/yellow/red) for a Job Site address on the map
- Job Site address: the street address to which the signal is attached
- Experience text: optional text descriptions and three job site condition indicators submitted by Verified Contractors. Author identity is shown as anonymous Verified ID only (e.g., Verified · #SP-XXXXXXXX) — business names, personal names, and logos are never displayed.

NEVER visible to anyone on the platform:

- Your name, photo, or personal contact information
- Your individual color assessment — only the aggregate combined signal is shown, not individual submissions
- The identity, name, or personal information of any Client associated with the address

StarProve does not collect or display any personal information about Clients. The platform is address-based. No Client database exists.

3.2 Service Providers

We may share information with third-party vendors who help us operate our business, including:

- Cloud hosting and data storage providers
- Analytics services (used in aggregate, anonymized form)
- Customer support platforms
- Identity verification services

These providers are contractually obligated to protect your information in accordance with applicable privacy laws, including 15 U.S.C. § 1681a and CCPA/CPRA requirements. We require all service providers to sign Data Processing Agreements (DPAs).

3.3 Legal Requirements

We may disclose information if required to do so by law or in response to valid requests by public authorities (e.g., a court order or government agency request), in accordance with applicable law.

3.4 Business Transfers

In the event of a merger, acquisition, or sale of all or a portion of our assets, your information may be transferred as part of that transaction. We will notify you via email and/or prominent notice in the App of any change in ownership or uses of your personal information.

4. YOUR CONTENT AND EXPERIENCES

The App allows Verified Contractors to submit address-based professional Experiences — a color assessment (green, yellow, or red) and an optional text description — tied to a specific Job Site address. No Client name or personal information is collected, stored, or displayed.

StarProve has a zero-tolerance policy for objectionable content or abusive users. By posting content, you agree to the following:

4.1 Responsibility for Your Posts

You are solely responsible for the content you post. You represent and warrant that your experiences are based on your honest, firsthand experience and are not false, misleading, or defamatory.

4.2 Prohibited Content

You may not post content that:

- Is knowingly false, misleading, or defamatory
- Contains threats, harassment, or personal attacks
- Includes obscene, vulgar, or hateful language
- Discloses private information (doxing), such as unlisted phone numbers, email addresses, or social security numbers
- Targets, identifies, or characterizes any individual person rather than job site conditions
- Evaluates or rates any individual person as opposed to professional working conditions at a job site address
- Discriminates against any person based on race, color, religion, sex, national origin, disability, familial status, or any other protected characteristic under applicable law
- Violates any applicable law or regulation

4.3 App's Role as a Host

In accordance with Section 230 of the Communications Decency Act (47 U.S.C. § 230), we are a provider of an interactive computer service. We are not liable for any offensive, inaccurate, or defamatory content posted by users, though we reserve the right to moderate content that violates our rules.

4.4 Aggregate Site Signal — Anonymous Address-Based Indicator

The Aggregate Site Signal is a single color indicator (green, yellow, or red) displayed on the map for each Job Site address. It is automatically calculated by combining all color assessments submitted by verified Contractors who have worked at that address. Key privacy features of this system:

- The signal is anonymous — no individual Contractor's assessment is displayed separately
- The signal is address-based — it is not associated with any named individual
- No Client personal data is collected, used, or displayed at any point in the process
- The signal represents collective subjective professional opinion and does not constitute a factual determination about any person or entity

4.5 Reporting Mechanism

Users can report any experience that violates these terms using the "Report" button available on each experience. All reports are reviewed within 24 hours.

4.6 User Blocking Mechanism

Users have the ability to block other users who engage in abusive behavior. When a user is blocked, they will no longer be able to view or interact with the blocking user's content.

4.7 24-Hour Response Commitment

Upon receiving a valid report of objectionable content through our reporting mechanism, we will review the reported experience within 24 hours, remove any content that violates these terms, and take appropriate action against the user who posted the violating content.

4.8 Dispute Process for Job Site Addresses

Because StarProve does not identify or display any Client by name or personal information, disputes are address-based, not person-based. A person or entity with a verified connection to a Job Site address may dispute the Aggregate Site Signal at that address. To do so, they must first register as a verified Contractor on the platform using their own professional credentials. Full details of the dispute process are set out in Section 9 of our Terms and Conditions. We will not remove or adjust a signal solely because it is unfavorable or because the property owner disagrees with the professional opinions expressed.

4.9 Removal of Content

We reserve the right, but have no obligation, to remove content that violates our rules. You can request the deletion of specific public experiences you have posted. However, removal from our App may not ensure complete removal, as we cannot control search engines or other third parties who may have copied that information.

5. CHILDREN'S PRIVACY

StarProve is not intended for individuals under the age of 18. This requirement applies to all users.

All users must be at least 18 years of age. By registering and using the App, you confirm that you are at least 18 years old.

We do not knowingly collect personal information from anyone under 18. If we discover that a user under 18 has accessed the platform, we will delete any associated data and block further access immediately.

Because our App is publicly downloadable, we rely on the following age enforcement mechanisms:

- App Store age rating: the App is rated 17+ in the Apple App Store, which activates Apple's parental control restrictions
- Terms acceptance: all users confirm they are 18+ by accepting these Terms
- KYC verification: professional documentation required for Verified Contractor status is issued only to adults aged 18+

In accordance with the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506, we do not knowingly collect personal information from children under 13. If you believe a minor has accessed the platform, please contact service@ivirgo.us immediately.

6. YOUR STATE PRIVACY RIGHTS

Residents of certain states may have additional rights regarding their personal information under state laws:

State	Law	Key Statute
California	California Consumer Privacy Act (CCPA) as	Cal. Civ. Code §§ 1798.100-1798.199

	amended by CPRA	
Colorado	Colorado Privacy Act (CPA)	Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313
Virginia	Virginia Consumer Data Protection Act (VCDPA)	Va. Code Ann. §§ 59.1-571 to 59.1-581
Connecticut	Connecticut Data Privacy Act (CTDPA)	Conn. Gen. Stat. §§ 42-515 to 42-525
Utah	Utah Consumer Privacy Act (UCPA)	Utah Code Ann. §§ 13-61-101 et seq.

These rights may include the right to:

- Know what personal information we have collected and how it has been used and shared
- Request deletion of your personal information
- Correct inaccuracies in your personal information
- Opt out of the "sale" or "sharing" of your personal information for cross-context behavioral tracking
- Data portability — receive your personal information in a machine-readable format
- Appeal (Colorado): Right to appeal our decision regarding your privacy request within 45 days

Note: StarProve does not sell or share personal information as defined by these laws. We do not use personal information for targeted advertising.

To exercise these rights, please contact us at service@ivirgo.us. We will process your verifiable request within the timeframe required by applicable law (typically 45 days under CCPA/CPRA, with a possible 45-day extension).

Do Not Sell or Share My Personal Information: Because we do not sell or share personal information for advertising purposes, a formal opt-out mechanism is not required. However, you may contact us at service@ivirgo.us at any time to request information about how your data is used.

7. DATA SECURITY AND RETENTION

7.1 Security Measures

We implement a variety of administrative, technical, and physical security measures designed to safeguard your personal information against unauthorized access, use, or disclosure. This includes secure data storage and encryption where appropriate, in accordance with FTC standards for data security under Section 5 of the FTC Act (15 U.S.C. § 45).

Ratings are aggregated and anonymized where possible to protect the identity of individual contractors while still providing valuable community insights.

7.2 Data Retention Schedule

Data Type	Retention Period

Work Category (Trade Type)	Retained for the duration of the account. Used solely for KYC license verification. Not displayed to other users.
Contractor ID (assigned at KYC verification)	Retained for the duration of the account. Used solely as anonymous identifier on Experiences. Not linked to any public profile.
Account data (Google/Apple/Email)	Retained for the duration of the account, plus 3 years after deletion. OAuth tokens are not stored — authentication handled by Google/Apple/email provider.
KYC-verified member Experience text	Retained while account is active; deleted within 30 days of account deletion request, subject to legal holds.
KYC verification result (verified/not verified + timestamp)	Retained 5 years from registration for fraud prevention and legal compliance. IVirgo LLC stores ONLY the verification result — no documents, no license numbers, no personal records.
KYC verification documents (originals)	NOT stored by IVirgo LLC. Reviewed and then permanently deleted (hard delete) by IVirgo LLC internal verification system immediately after the verification decision.
Device / usage data	Retained for 24 months in aggregate/anonymized form only.
Communications / support	Retained for 3 years from last interaction.
Confidentiality acknowledgment logs	Retained for 5 years in append-only storage (user hash, acknowledgment version, timestamp, device fingerprint).

7.3 Data Breach Notification

In the event of a data breach involving your personal information, we will notify affected users in accordance with applicable law, including the New Jersey Identity Theft Prevention Act (N.J.S.A. 56:8-163) and similar state laws. Notification will be provided:

- Via email to the address associated with your account
- Via in-app notification
- In the most expedient time possible and without unreasonable delay

For questions about security incidents, please contact service@ivirgo.us.

8. THIRD-PARTY SERVICES AND SDK DISCLOSURE

Our App may use the following third-party services. Each has its own privacy policy governing the use of your information:

Service	Purpose	Privacy Policy
Apple Maps / Google Maps SDK	Map display for job site addresses	apple.com/privacy / policies.google.com
Google Sign-In (OAuth 2.0)	Account authentication. IVirgo LLC receives only: unique user ID, name, email address.	policies.google.com/privacy
Apple Sign-In (Sign in with Apple)	Account authentication. IVirgo LLC receives only: unique user ID, name, email (or relay email).	apple.com/privacy
Cloud Hosting (e.g., AWS or similar)	Secure data storage	Available upon request
Analytics (aggregate only)	App improvement, crash reporting	Data anonymized before processing
IVirgo LLC Internal Verification System	Automated identity and credential verification. Documents encrypted in transit, reviewed, then permanently deleted (hard delete).	ivirgo.us/privacy

We do not use advertising SDKs or share data with ad networks. StarProve does not serve advertising of any kind. We do not use tracking SDKs that monitor your behavior across other apps or websites.

8.1 Identity Verification (KYC) — Detailed Disclosure

Because StarProve requires verification of professional credentials for all contractors, we rely on an internal identity and credential verification system. This section provides the detailed disclosure required by applicable state privacy laws.

What We Send to the Verification System

When you register or re-verify your account, we transmit the following:

- Images or scans of the professional document(s) you submit (e.g., contractor license, business license, insurance certificate, trade certification)
- Your name as entered during registration, for matching against document data
- A unique session identifier assigned by StarProve (not your account ID)

What the Verification System Returns to Us

- Verification result: pass, fail, or pending manual review
- Document type confirmed: category of document verified
- Confidence score: an automated authenticity score (numeric)
- Timestamp: date and time of verification

- Reason code (if failed): category of failure (e.g., "document expired," "document not recognized")

What IVirgo LLC Stores

IVirgo LLC does NOT store copies of your original identity documents, license images, or scans on our servers. We store ONLY the verification result, document type, confidence score, and timestamp. Your actual documents are permanently deleted (hard delete) immediately after the verification decision.

Your Rights Regarding KYC Data

Upon account deletion, IVirgo LLC will delete the verification result data we hold (result, document type, timestamp). Note: Deletion of verification data may result in loss of your verified status and require re-verification if you wish to continue using StarProve.

9. PUSH NOTIFICATIONS

StarProve may send push notifications to your device for the following purposes:

- New experiences posted about job sites you follow
- Account security alerts (e.g., login from new device)
- App updates and important service announcements
- Dispute and moderation updates related to your content

Push notifications are requested through the standard iOS permission dialog. You can manage or disable push notifications at any time in your iOS Settings → Notifications → StarProve.

We do not send marketing or promotional push notifications without your explicit opt-in consent.

10. COOKIES AND SIMILAR TECHNOLOGIES

The StarProve mobile App does not use traditional browser cookies. However, we may use the following technologies:

- Local device storage: To remember your login session and app preferences.
- Analytics identifiers: Anonymized identifiers used to understand aggregate usage patterns. These are not used for advertising or cross-app tracking.

We do not use advertising cookies, tracking pixels, or any technology that monitors your behavior outside of the StarProve App.

11. ACCESSIBILITY

IVirgo LLC is committed to making StarProve accessible to users with disabilities. We strive to conform to the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards, as recommended by Apple's Human Interface Guidelines.

If you experience any accessibility issues with our App, please contact us at service@ivirgo.us and we will make reasonable efforts to address your needs.

12. FAIR CREDIT REPORTING ACT (FCRA) — IMPORTANT NOTICE

StarProve is NOT a consumer reporting agency as defined by the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.). All information on the App is based solely on the firsthand transactions and experiences of its users, which is expressly excluded from the definition of a "consumer report" under 15 U.S.C. § 1681a(d)(2)(A).

You may not use information from StarProve for purposes covered by FCRA, including employment screening, tenant screening, or credit decisions, without our express written consent.

12.A INTERNATIONAL EXPANSION — PRIVACY FRAMEWORK

StarProve is currently a U.S.-only platform. This section describes how our Privacy Policy will evolve when IVirgo LLC expands to new markets. When a regional launch occurs, a country-specific Privacy Addendum will be published and incorporated into this Policy by reference. Until then, this Policy applies in its U.S.-only form.

12.A.1 Canada — Privacy Framework (Reserved)

CANADA PRIVACY ADDENDUM — PLACEHOLDER. Governing law: PIPEDA (federal) + Quebec Law 25. Privacy Officer: To be designated at launch. Breach notification: 72 hours to Office of the Privacy Commissioner (OPC) and provincial equivalents.

12.A.2 European Union / EEA — Privacy Framework (Reserved)

EU/EEA PRIVACY ADDENDUM — PLACEHOLDER. Governing law: GDPR (Regulation (EU) 2016/679). Data Protection Officer (DPO): To be designated. EU Representative (Art. 27): To be designated.

12.A.3 United Kingdom — Privacy Framework (Reserved)

UK PRIVACY ADDENDUM — PLACEHOLDER. Governing law: UK GDPR + Data Protection Act 2018. UK Representative (Art. 27 UK GDPR): To be designated. ICO Registration: Required before UK launch.

12.A.4 Australia — Privacy Framework (Reserved)

AUSTRALIA PRIVACY ADDENDUM — PLACEHOLDER. Governing law: Privacy Act 1988 (Cth) + Australian Privacy Principles (APPs). Notifiable Data Breaches (NDB) scheme: Notification to OAIC and affected individuals required.

12.A.5 Addendum Publication Process

When IVirgo LLC is ready to launch in a new region, the relevant Privacy Addendum will be finalized and published at least 30 days before regional launch. Users in that region will receive email and in-app notification of the new Addendum. Continued use after the effective date constitutes acceptance.

13. CHANGES TO THIS PRIVACY POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by:

- Posting the new Privacy Policy on this page and updating the "Last Updated" date
- Sending an email notification to your registered email address for material changes
- Displaying a prominent in-app notification for material changes

For material changes, we will provide at least 30 days' advance notice before the changes take effect.

Your continued use of the App after any changes constitutes your acceptance of the new Privacy Policy.

14. CONTACT US

Email	service@ivirgo.us
Company	IVirgo LLC
Address	54 Eastgate Ln, Willingboro, New Jersey 08046, USA

This Privacy Policy was last reviewed and approved by IVirgo LLC on April 1, 2026.
StarProve Privacy Policy — IVirgo LLC | v12 (Revised — Single-Tier KYC Model)