GTA TECHNOLOGY, LLC

PRIVACY POLICY
Last updated: October 16, 2025

---

1. Introduction

This Privacy Policy explains how **GTA Technology, LLC** ("**GTA Technology**," "**we**," "**us**," or "**our**") collects, uses, discloses, and protects information in connection with its software and platforms, including the **Protect by GTA** client application (the "Client App"), the **Protect Advisor by GTA** application (the "Advisor App"), the **Arti Assist** application, and related websites and services (collectively, the "**Services**").

This Policy applies to all platforms and websites operated by GTA Technology, LLC, including the Protect by GTA mobile app, the Protect Advisor by GTA mobile app, the Arti Assist application, the ProtectGTA.com web application, the ProtectGTA.com website, and the GTA-Technology.com website.

Protect and Arti Assist are United States–based platforms that help licensed insurance advisors and their clients manage documents, coverage information, asset inventories, and compliance workflows. GTA Technology operates these platforms as a consultant and service provider and is not an insurance agent, producer, or carrier.

---

2. Information We Collect

We collect account details such as name, email, phone, and roles, along with messages and materials you upload, including policies, contracts, receipts, invoices, financial statements, photographs, and claims documentation.

You may also list assets in detail, including descriptions, categories, serial numbers, receipts, attachments, and photographs. These inventories help validate insurance coverage for advisors and provide personal recordkeeping for clients in the event of a loss.

If you upload a government-issued ID, for example a driver's license, passport, or Social Security document, Protect uses AI to detect and redact sensitive identifiers before any information is stored in our systems. We do not store full federal ID numbers or Social Security numbers.

We may retain limited non-sensitive data such as name, address, and expiration date to validate records and generate risk alerts, for example an approaching ID expiration. The full ID image remains on your device and is not stored in our systems.

If you use biometric unlock on your device (for example Face ID or Touch ID), the biometric template remains on your device and is never shared with us.

Protect operates as an extension of your agency management system ("AMS"). Advisor and broker access to client data in Protect is defined entirely by the AMS security profile. If an advisor or broker has access to a client's account or policy in the AMS, they will have the same level of access in Protect. Protect does not independently assign or modify advisor permissions.

Clients can invite delegates such as family members, accountants, or attorneys and can configure delegate access directly in the app. Delegates can only view or upload information as permitted by the client. This model ensures that advisor access follows agency compliance rules while clients maintain control over their personal sharing.

As part of onboarding, Protect connects directly to your agency's AMS and imports client, policy, and related operational data needed to provide the Services. Protect also connects to carrier portals and document systems where available.

Protect uses public and syndicated data sources to enrich records and identify risk. Examples include ATTOM property, tax, and characteristics data, and public sources such as NOAA, FEMA, and county assessor or recorder records.

Protect does not pull consumer financial data beyond what exists in the AMS, such as policy financials and billing information, and does not access or store bank account numbers, credit card numbers, credit scores, payroll totals, or income data.

We also collect limited technical information such as device type, operating system, app version, log files, diagnostics, and in-app actions (for example document views or deliveries) to secure and improve the Services. We do not collect precise geolocation unless you enable a feature that requires it.

---

3. How We Use Information

We use collected information to provide, operate, and secure the Services; generate and reconcile insurance documentation such as ACORD forms and COIs; enable secure document access and inventory tools; support claims-related submissions; enrich records with public and third-party data; generate compliance alerts, Smart Reports, and risk

insights; maintain immutable audit trails for compliance and E&O defense; provide clients with recordkeeping and loss documentation tools; and improve platform functionality, reliability, and user experience.

---

4. GLBA and U.S. Financial Privacy

When Protect processes nonpublic personal information on behalf of an advisor or agency, we do so as a service provider under the Gramm–Leach–Bliley Act (GLBA). We implement administrative, technical, and physical safeguards consistent with the GLBA Safeguards Rule.

Protect operates under the Gramm–Leach–Bliley Act (GLBA) and is therefore exempt from most U.S. state consumer data privacy statutes, including the California Consumer Privacy Act (CCPA) and similar state laws.

---

5. How We Share Information

We share information with trusted vendors that help operate the Services, such as AWS for hosting, Stripe for payments, vetted large language model providers for AI processing, analytics, diagnostics, and customer support tools.

Protect uses public and syndicated data aggregators such as ATTOM to enrich property and risk information. We do not sell personal data to these providers or any other third party.

Data may be shared with your advisor and any delegates according to the permissions configured by the AMS or by you in the Protect app.

We may disclose information to comply with law, respond to lawful requests, protect rights or safety, or enforce our Terms.

If GTA Technology engages in a merger, acquisition, or financing, information may be transferred subject to confidentiality protections.

---

6. Payments

Payments for subscriptions and services are processed by secure third parties such as Stripe. Protect does not store full payment card numbers. Your use of payment services is governed by the processor’s terms and privacy policy.

---

7. Security

Protect uses administrative, technical, and physical safeguards, including encryption in transit and at rest, hosted on AWS enterprise-grade infrastructure.

AI is used to detect sensitive identifiers and enforce redaction so full federal IDs and Social Security numbers are never stored.

No system can be guaranteed 100% secure. You are responsible for protecting your devices and credentials.

---

8. Retention

We retain data as long as needed to provide the Services and meet legal obligations.

Audit-grade logs and records required for compliance or E&O defense are retained for seven years.

When a user deletes their account, Protect permanently deletes all user-provided data such as uploads, inventories, photos, and attachments. Only legally required audit logs remain.

Deletion is immediate and irreversible. If an account is later reinstated, AMS data will repopulate automatically but any manually uploaded data will not be recoverable.

If an account is suspended for nonpayment, Protect retains user-provided data for 30 days. After that, all uploaded data is deleted permanently except legally required records.

If the account is reactivated after deletion, AMS data will repopulate automatically but uploaded data will not be recoverable.

Records are retained not only for compliance but also to support discovery and legal defense in the event of lawsuits or disputes. These logs serve as neutral evidence intended to protect both advisors and clients by maintaining an accurate, immutable history of actions and communications.

---

9. Your Rights and Choices

You can view and edit your data while your account is active. When you delete your account, Protect permanently deletes all user-provided data, retaining only legally required logs. No contact is necessary.

If you reinstate your account, AMS data will repopulate automatically but deleted uploads will not return.

Advisor and broker access in Protect is defined by the AMS security profile. Clients control permissions for their delegates inside the Protect app.

You can also manage local device permissions such as camera or file storage.

Protect does not use in-app third-party advertising. You may opt out of non-essential emails through unsubscribe links.

---

10. International Users and U.S. Processing

Protect is hosted in the United States. If you access the Services from outside the United States, you consent to U.S. processing and data storage.

Foreign clients with U.S.-based assets or insurance who are invited to use Protect by their advisor agree to this processing by using the Services.

---

11. Children's Privacy

Protect is not designed for children under 18. Users must be 18 or older to register directly.

A client or advisor may invite individuals 16 or older who are insured under an active policy, provided the invitation is made by a parent, guardian, or advisor.

Access for such users is limited to necessary insurance functions such as viewing ID cards or contributing to inventories. Protect is not intended for users under 16 and does not knowingly collect their information.

---

12. Data Use and State Privacy Notice

Protect does not sell, rent, or share personal information.

While state privacy laws such as the CCPA grant consumers certain rights, data processed by Protect is regulated under the GLBA Safeguards Rule and is therefore exempt from those state statutes.

We nonetheless honor equivalent rights of access, correction, and deletion as a matter of policy. We do not share data for marketing or cross-context behavioral advertising.

Personal information is used only to provide the Services, including account authentication, security, compliance, and support.

Protect honors all applicable state privacy rights such as access, correction, and deletion and will not discriminate against users who exercise them.

Protect users may contact **privacy@gta-technology.com** to exercise any rights under applicable state or federal privacy law.

---

13. AI and Automated Processing

Protect uses both proprietary artificial intelligence (AI) and vetted external large language models (LLMs) to deliver and improve the Services.

AI transforms, summarizes, classifies, and validates text and documents, detects sensitive identifiers, and enforces redaction so full federal ID and Social Security numbers are never stored.

Protect's AI continuously reviews publicly available and licensed data from local, state, federal, and carrier sources to identify potential new risks or regulatory changes that could impact clients and advisors.

AI systems may prioritize and present risk insights in plain language to help users better understand exposures and next steps.

All AI-generated insights are informational only and require advisor review before use in client or business decisions.

---

14. Cookies and Analytics

Protect apps do not use third-party advertising SDKs.

Our websites may use first-party cookies and analytics to understand usage patterns and improve performance.

Users can control cookie settings in their browser.

---

15. Changes to This Policy

We may update this Privacy Policy periodically.

Material changes will be communicated through the apps or by email when appropriate.

Continued use of the Services after an update constitutes acceptance of the revised Policy.

---

16. Contact Us

GTA Technology, LLC
365 5th Ave. S, Suite 240
Naples, Florida 34102
Email: **privacy@gta-technology.com**