GTA TECHNOLOGY, LLC

PRIVACY POLICY
Last updated: March 18th, 2026

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 or other sensitive document, including a driver's license, passport, tax document, legal record, or similar file, Protect may securely store that document to enable cross-device access, recordkeeping, and controlled sharing within the platform.

Protect does not modify, redact, or alter user-uploaded documents. Documents are stored as provided by the user and are accessible only in accordance with AMS-based

authorization, platform role controls, and user-configured sharing settings as described in this Policy.

Users are responsible for determining what information they choose to upload, store, and share within the platform, including any sensitive personal, financial, legal, or business information. Users are also responsible for managing access permissions and should carefully consider what information is shared and with whom.

Protect may use uploaded information to classify documents, organize records, generate alerts, and create risk insights or other service outputs. While such outputs may be informed by user-uploaded or user-entered information, Protect is designed not to expose full sensitive identifiers, such as full government ID numbers or full Social Security numbers, in ordinary service outputs where they are not required. Such outputs may be made available to both the client and the advisor as part of the Services, even where the underlying client-entered documents or records are not separately shared in full.

Protect does not actively review or monitor user-uploaded content except as needed to provide, secure, maintain, support, or improve the Services, enforce our terms, comply with law, or respond to user requests.

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 integrates with your agency management system ("AMS") and uses AMS security profiles to determine which advisors and broker personnel are authorized to access a particular client relationship within Protect. If an advisor or broker does not have access to a client relationship through the AMS security profile, that individual will not have access to that client's information in Protect.

For advisors and broker personnel who are authorized through the AMS, access to AMS-derived data within Protect follows the applicable AMS security profile. Access to client-entered data within Protect, including uploaded documents, IDs, assets, inventories, and other user-provided information, is subject to an additional layer of client-controlled permissions within the platform. In other words, an advisor must first be authorized through the AMS and, where applicable, must also be granted access by the client to view client-entered information.

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 allows clients to control delegate access directly while advisor and broker access continues to follow AMS-based authorization

together with any additional client-controlled sharing settings applicable to client-entered information.

Protect uses multiple categories of data within the Services. Some information is imported from the AMS or other connected systems and is governed by those authorization models. Other information is entered or uploaded directly by the client and remains subject to client-controlled sharing settings. Protect may also generate alerts, reports, recommendations, Smart Reports, and risk insights based on AMS data, client-entered data, public records, third-party data, or any combination of those inputs.

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. SMS Authentication Messages

Protect may send one-time password (OTP) authentication codes to the mobile phone number associated with your account to verify your identity and protect account access.

By providing your mobile phone number within the Protect platform, you consent to receive SMS messages used solely for login authentication and account security.

Message frequency depends on login activity or verification requests. Standard carrier message and data rates may apply.

You may opt out by replying **STOP** to any authentication message. Reply **HELP** for assistance. Please note that opting out may prevent you from accessing **your account or certain features that require SMS verification**.

Protect uses mobile numbers only for authentication and security purposes and does **not use or share mobile numbers for marketing or promotional communications**.

For questions regarding SMS communications, contact: **privacy@gta-technology.com**

4. How We Use Information

We use collected information to provide, operate, secure, support, and improve the Services; generate and reconcile insurance documentation such as ACORD forms and COIs; enable secure document access, inventory tools, and personal or business recordkeeping; support claims-related submissions; enrich records with public and third-party data; generate compliance alerts, Smart Reports, recommendations, and risk insights; maintain audit trails for compliance, E&O defense, and operational integrity; and improve platform functionality, reliability, accuracy, and user experience.

Certain alerts, reports, recommendations, Smart Reports, and risk insights may be generated from AMS data, client-entered data, public records, third-party data, or a combination of those sources, and may be made available to both the client and the advisor as part of the Services even where the underlying client-entered documents or records are not separately shared in full.

5. 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.

6. 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 to enrich property and risk information. We do not sell personal data to these providers or any other third party.

Information may be made accessible to advisors, broker personnel, delegates, and other authorized users based on the type and source of the information and the applicable authorization model.

AMS-derived data is shared in accordance with the applicable AMS security profile and related advisor-client relationship.

Client-entered data, including uploaded documents, IDs, assets, inventories, and other user-provided information, is shared only in accordance with the permissions configured by the account owner within Protect and, where applicable, only with advisors or broker personnel already authorized through the AMS.

Protect may also share alerts, reports, recommendations, Smart Reports, and risk insights generated from AMS data, client-entered data, public records, third-party data, or a combination of those sources with both the client and the advisor as part of the Services. Such outputs are part of the platform's core functionality and are not necessarily limited by whether the underlying client-entered source material has been separately shared in full.

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.

7. 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.

8. Security

Protect uses administrative, technical, and physical safeguards designed to protect information handled through the Services, including encryption in transit and at rest, permission-based access controls, role-based restrictions, authentication controls, audit logging, and AWS-hosted enterprise-grade infrastructure.

Access to production systems and user data is restricted to authorized personnel and is subject to logging, monitoring, and internal access controls.

Protect's security model distinguishes among AMS-derived data, client-entered data, and system-generated outputs. Access is governed through a combination of AMS authorization, platform role controls, and user-configured sharing settings, depending on the type of information involved.

Protect may use automated tools, including AI and related technologies, to classify, organize, analyze, and protect information and to support alerts, recommendations, and risk insights. Protect is designed to limit unnecessary exposure of highly sensitive identifiers in ordinary service outputs where such identifiers are not required.

No system can be guaranteed 100% secure. Users are responsible for protecting their devices, credentials, and any access they grant to others.

8A. Sensitive Information and User Responsibility

Protect may be used to store sensitive personal, financial, legal, business, and insurance-related documents and information.

Users are responsible for determining what information they upload, store, enter, and share within the platform, including any sensitive personal, financial, legal, or business information.

Users are also responsible for managing sharing settings and access permissions for delegates and for any client-entered information they choose to make available through Protect.

Protect does not verify the identity, authority, or legal status of any delegate or other person granted access by the user and is not responsible for how information is used once access has been granted by the account owner or other authorized user.

Users acknowledge that once access is granted to any advisor, delegate, or third party, Protect does not control how such information is further used, retained, or shared by that party.

9. 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.

10. 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 to AMS-derived information in Protect is governed by the AMS security profile. Clients control permissions for delegates and for client-entered information shared within Protect, subject to the platform's authorization model.

Users are responsible for managing sharing settings and access permissions for delegates and for any client-entered information they choose to make available through the platform.

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.

11. 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.

12. 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.

13. 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.

14. 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 may transform, summarize, classify, organize, validate, and analyze text, documents, and records to deliver and improve the Services, support document handling, identify issues, and generate alerts, recommendations, Smart Reports, and risk insights. AI and related automated processes may also be used to help identify and limit unnecessary exposure of highly sensitive identifiers in ordinary service outputs where such identifiers are not required.

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.

15. 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.

16. 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.

17. Contact Us

GTA Technology, LLC
365 5th Ave. S, Suite 201
Naples, Florida 34102
Email: **privacy@gta-technology.com**