

Altumint Program Guidelines on Data Privacy

Purpose

This Policy defines how Altumint collects, protects, and destroys data in the automated traffic safety programs we operate with our government safety partners, and applies to every Altumint program in every jurisdiction. Our programs serve a single purpose: traffic safety. Altumint captures and retains vehicle images and data only when a potential violation is detected. For all other vehicles, no images, video, license plate information, or registered-owner information are retained or transmitted.

Guiding Principles

1. **Single Purpose Traffic Safety Cameras with no Integration of other Technologies**

Altumint's speed and red-light cameras are used solely for traffic safety programs. Our systems operate independently of other enforcement or surveillance technologies, and we bid only on programs consistent with that standard. Altumint does not and will not integrate our technology, data, or infrastructure for any other third-party purpose such as automated license plate readers (ALPR) or sound detection technology.

2. **Vehicle-Based Identification Only with No Facial Recognition or Driver Identification Programs.**

Altumint identifies vehicles through license plates and registered-owner records, and our technology is designed so that drivers and occupants remain unidentified. Facial recognition, biometric identification, and driver-identification photography are outside the scope of every Altumint program, and we bid only on programs consistent with that standard.

3. **Protecting Individual Identities**

The System collects only what is necessary to identify a violating vehicle and support a citation. Program data is used to administer and adjudicate traffic violations, and cross-referencing with external databases occurs only where specifically authorized and necessary for that purpose. Surveillance, profiling, marketing, tracking, and commercial analytics uses are prohibited.

4. **Data Retention Limits**

Recorded vehicle data is retained only as long as necessary to complete the citation, adjudication, and appeal process, and in accordance with state and local retention rules. Where the law sets no specific period, Altumint's automated default destroys data within 30 days of citation resolution by payment or dismissal. Data from events rejected before citation is destroyed within 30 days, or sooner where required by law.

5. **Role-Based Access Control (RBAC)**

Access to Program data is limited to authorized personnel based on job responsibilities. Altumint personnel are subject to authentication, training, screening, and access-management requirements, with access reviewed and revoked when no longer required under the authority of our Chief Technology Officer. Each Safety Partner identifies its authorized users, ensures they meet applicable training and agency requirements, and notifies Altumint promptly when access should change. Partner access is documented in Business Rules signed by both parties.

6. Data Security and Sensitive Information Violation images and data are encrypted at the time of capture and stored in accordance with recognized standards for securing legal evidence. Violation notices are issued without Social Security numbers, which are excluded from the Program entirely.

7. Disclosure Only as Authorized with No Sale, Monetization, or Unauthorized Disclosure of Program Data.

Program data is shared only with authorized service providers working on behalf of Altumint or our Safety Partners, or in response to valid legal processes such as a specific, particularized warrant or court order. Altumint's sole revenue from Program data is the operation of the safety program itself; the sale, licensing, or monetization of personal data is prohibited.

8. Law Enforcement and Government Data Requests

Disclosure to other law enforcement or federal agencies requires a specific, individualized, and legally valid compulsory order. Every such request is escalated to Legal Counsel and the deploying government safety partner before any response.

9. Definition and Protection of Personally Identifiable Information

PII includes, where collected, the vehicle owner's address, telephone number, license plate number, photograph, financial-account or payment-card information, and the date, time, location, or direction of travel. PII is disclosed, stored, and retained only as necessary to charge, collect, and enforce fines. Where records are subject to a public-records law, only non-PII data may be disclosable.

Legal Basis and Jurisdictional Authorization

Altumint deploys automated traffic safety programs only where:

- The state or local government has enacted specific legal authorization for automated speed, red-light, or school bus enforcement;
- The deployment has received all required regulatory approvals (e.g., state DOT sign-off, local ordinance, public hearing where required);
- Camera locations, enforcement hours, and violation thresholds fall within the bounds of that authorization; and
- The program operates on a standalone basis, with no required integration of our data, enforcement technology, or infrastructure with unrelated third parties, vendors, or uses.

Governance and Oversight

Oversight of this Policy is assigned to the CAO of Altumint. Governance includes:

- Data Destruction Report to the Board
- Client Certification Report
- Board confirmation of the compliance standards in Appendix A
- Annual review of this Policy
- Annual Review of Altumint's internal audits confirming compliance with this Policy and its data-handling requirements
- Public posting of this Policy on Altumint's website

Appendix A: Compliance Standards and Certifications

Altumint maintains the following independent certifications and partnerships, which the Board confirms annually.

SOC 2 Type II Compliance

SOC 2 is a control framework created by the American Institute of Certified Public Accountants (AICPA) evaluating controls for security, availability, processing integrity, confidentiality, and privacy. Altumint earns and retains this compliance annually through an audit by an independent CPA firm.

CJIS Compliance

The FBI's Criminal Justice Information Services (CJIS) Security Policy governs how law enforcement, government agencies, and third-party vendors access, store, transmit, and destroy Criminal Justice Information. Altumint's CJIS requirements include multi-factor authentication for all users, fingerprinting of users with access to enforcement data, and restricted access. All Altumint employees complete CJIS training at hire and annually thereafter.

Nlets Strategic Partnership

Nlets, the International Justice and Public Safety Network, requires its partners to complete rigorous technical and financial vetting, pass a comprehensive security audit before connectivity, and secure formal board or committee approval. Altumint has completed this process and maintains the partnership.

State and Local Law Compliance

Altumint operates only in states with authorizing language and monitors and complies with all state and local data protection laws and regulations in each jurisdiction we serve. Altumint's data protection practices are designed to meet or exceed the requirements of local governing law.