

Altumint Program Data Privacy Policy

Overview and Purpose

This policy governs how Altumint designs, deploys, and operates automated traffic safety programs. Altumint continues to recognize our responsibility in working with our safety partners to ensure that our safety program respects all individual privacy rights. Included in Altumint's policy is the handling of any personal information obtained, access to data, and professional standards and audits.

With intention, Altumint has pursued and obtained several objectives to help ensure our standards of conduct and data protection and integrity are in line with nationally recognized standards. Among those are:

SOC 2 Type II Compliance

SOC 2 is a control framework created by American Institute for Certified Public Accountants (AICPA). The Trust Services Criteria is used for attestation or consulting engagements to evaluate controls relating to security, availability, processing integrity, confidentiality, and privacy. Compliance is designed to prove Altumint safely manages and protects user data and requires an audit by an independent Certified Public Accountant (CPA). This compliance must be earned and retained on an annual basis.

Nlets Strategic Partnership

The International Justice and Public Safety Network requires their partners to undergo a rigorous technical and financial vetting process, pass a comprehensive security audit before connectivity, and secure formal board or committee approval.

CJIS Compliance

The Criminal Justice Information Services (CJIS) is an FBI Division, and the CJIS Security Policy is a mandatory set of security standards established by the FBI. It governs how law enforcement, government agencies, and third-party vendors access, store, transmit, and destroy Criminal Justice Information (CJI). Among the requirements of Altumint are multi-factor authentication for all Altumint users, fingerprinting authorized users with access to enforcement data, and restricted access. This is an ongoing process for Altumint new hires and requires annual participation from all Altumint employees.

State and Local Law Compliance

Altumint recognizes that our programs only operate in states that have authorizing language. We continue to monitor and comply with all state and local laws and regulations as it relates to data protection for their citizens. In most, if not all, states, Altumint engages in data protection practices that meet or exceed the legal requirements of local governing laws.

Altumint does not use Program data to construct vehicle movement histories, travel profiles, location histories, behavioral profiles, or databases designed to determine where an individual or vehicle has traveled. Altumint has not and does not provide customers or third parties with functionality designed for those purposes.

First and foremost, for vehicles for which no potential violation is detected, Altumint does not retain or transmit any vehicle images, video, license plate information, or registered-owner information.

For vehicles that exceed speed thresholds or run red lights, Altumint continues to recognize our responsibility in working with our safety partners to ensure that our safety program respects all individual privacy rights.

The purpose of this Data Privacy Policy (this “Policy”) is to define Altumint’s approach to integrating the consideration of privacy factors and state and municipal rules into our safety program.

Guiding Principles

Limited Data Collection.

Our safety program focuses on capturing and providing evidence only when a speeding threshold has been exceeded or a red-light violation has occurred. Altumint does not cross-reference Program data with external databases except as specifically authorized and necessary to administer or adjudicate a traffic violation. Program data will not be combined with external information for surveillance, profiling, marketing, commercial analytics, or *tracking*.

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

Altumint’s speed and red-light cameras have, and will, only be used for traffic safety programs. Altumint will not integrate our technology or data for any other purpose such as automated license plate readers (ALPR) or sound detection technology. Altumint will not permit co-location or integration of surveillance/enforcement technologies. Altumint will not bid on or participate in programs with a requirement for integration of other technologies or vendors with other purposes.

2. No Facial Recognition or Driver Identification Programs.

Altumint does not use facial recognition, biometric identification, driver-identification photography, or other technology designed to establish the identity of a vehicle’s driver or occupants. Altumint will not bid on or participate in programs requiring a positive identification of the driver with video or photographs.

3. Protecting Individual Identities.

The System will collect only what is necessary to identify a speeding vehicle and support a citation — not to identify, profile, or track individual people or to track non-offenders.

4. Data retention limits

Recorded vehicle data will be retained only as long as necessary to complete the citation, adjudication, and appeal process and according to state and local data retention rules. If there are no data retention restrictions required by law, Altumint’s automated, scheduled default maximum retention is 30 days from the date of resolution of the citation by payment or dismissal. If a violation does not become a

citation through a rejection, all data will be destroyed within 30 days or sooner if required by law.

5. Role-Based Access Control (RBAC)

Altumint employees and safety partners follow strict protocols limiting access to data. Altumint personnel. Access to Program data is limited to authorized Altumint personnel based on job responsibilities and approved access requirements. Altumint personnel are subject to applicable authentication, training, screening, and access-management requirements. Internal access is reviewed and revoked when no longer required. Safety partner personnel. Each Safety Partner is responsible for identifying the personnel it authorizes to access the Program and for promptly notifying Altumint when access should be added, modified, or removed. Safety Partners are also responsible for ensuring that their authorized users satisfy applicable training, qualification, and agency requirements. Authorization for access for Altumint employees will be held by the office of our Chief Technology Officer. Our safety partners' access will be documented by established Business Rules signed and authorized by Altumint and the Safety Partner's Project Manager or Executive.

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. Social Security numbers are never used, linked to names, or printed on violation notices.

7. No Sale, Monetization, or Unauthorized Disclosure of Program Data.

Altumint will never sell, license, or otherwise monetize personal data collected through the Program. Altumint will never share data with any third party except authorized service providers working on behalf of Altumint or our Safety Partners or when compelled by valid legal process (e.g., a specific, particularized warrant or court order).

8. Law Enforcement and Government Data Requests

Altumint will not proactively share, bulk-transfer, or provide standing access to program data to other law enforcement agencies or federal agencies absent a specific, individualized, and legally valid compulsory order. Requests of this nature must be escalated to Legal Counsel and the deploying government safety partner before any response.

9. Definition and Protection of Personally Identifiable Information.

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. Where records are subject to a public-records or freedom-of-information law, non-PII data may be disclosable; PII will not be disclosed, stored, or retained except as necessary to charge, collect, and enforce fines.

Legal Basis and Jurisdictional Authorization

Altumint will only deploy automated traffic safety programs in a jurisdiction if:

- The relevant state or local government has enacted specific legal authorization for automated speed red light enforcement;
- The deployment has received all required regulatory approval (e.g., state department of transportation sign-off, local ordinance, public hearing where required).
- Camera locations, enforcement hours, and violation thresholds fall within the bounds of that authorization.
- No integration of our data, enforcement technology, or infrastructure is required with an unrelated third party, other vendor, or use.

Our internal governance procedures to ensure that we adhere to this policy include:

- Oversight is assigned to Cory Battin, CFO of Altumint
- Board Monitoring
 - Monthly Data Destruction Report
 - Annual Confirmation
 - SOC 2 Compliance
 - Nlets Partnership
 - CJIS Training
 - Annual Review of Data Privacy Policy
 - Review of Altumint's internal audits to confirm compliance with this Policy and its data-handling requirements.
- Public Posting of Privacy Policy on Altumint's Website
- Monthly Client Certification Report