

Altumint Program Policy on Data Privacy

Frequently Asked Questions

This FAQ document explains Altumint's privacy policy in straightforward language. It is intended to help members of the public, government safety partners, policymakers, and other stakeholders understand what information Altumint collects, how it is used, and the limits Altumint places on its traffic-safety technology.

1. What is Altumint's privacy policy designed to do?

It explains how Altumint handles information in its automated traffic safety programs. The policy covers what data may be collected, who may access it, how it is protected, how long it is kept, and how Altumint limits the use of its technology and data.

2. Does Altumint collect information about every vehicle that passes a camera?

No. If no potential traffic violation is detected, Altumint does not retain or transmit vehicle images, video, license plate information, or registered-owner information.

3. When does Altumint retain information about a vehicle?

Altumint's safety programs focus on evidence associated with a potential traffic violation, such as exceeding an applicable speed threshold or running a red light. The information is used to support the traffic-enforcement process only.

4. Does Altumint track where vehicles or people travel?

No. Altumint does not use program data to create vehicle movement histories, travel histories, location histories, behavioral profiles, or databases designed to show where a person or vehicle has traveled.

5. Are Altumint's traffic cameras used as automated license plate readers (ALPRs)?

No. Altumint's speed and red-light cameras are single-purpose traffic safety cameras. Altumint will not integrate its technology or data with ALPR technology.

6. Can Altumint combine photo enforcement with sound cameras or other surveillance technology?

No. Altumint's policy prohibits integration with sound-detection technology and other unrelated surveillance or enforcement technologies. Altumint will not permit co-location or integration of those technologies and will not participate in programs that require such integration.

7. Can Altumint's camera infrastructure be connected to another vendor's unrelated technology?

No integration of Altumint data, enforcement technology, or infrastructure may be required with an unrelated third party, vendor, or use. Altumint will not bid on or participate in programs that require integration with technologies or vendors serving other purposes.

8. Does Altumint use facial recognition?

No. Altumint does not use facial recognition, biometric identification, or other technology designed to identify the driver or occupants of a vehicle.

9. Does Altumint photograph drivers to prove who was driving?

No. Altumint will not participate in programs requiring positive identification of a driver through photographs or video.

10. What personal information may be involved in a traffic-enforcement case?

Depending on the program and the information needed to administer a citation, personally identifiable information may include a vehicle owner's address, telephone number, license plate number, photograph, payment information, and information such as the date, time, location, or direction of travel.

11. Does Altumint combine traffic-enforcement data with other databases?

Altumint does not cross-reference program data with external databases except when specifically authorized and necessary to administer or adjudicate a traffic violation. The data is not to be combined with outside information for surveillance, profiling, marketing, commercial analytics, or tracking.

12. How long does Altumint keep violation data?

Altumint keeps recorded vehicle data only as long as necessary for the citation, adjudication, and appeal process and as required by state or local law. If the law does not set a retention period, Altumint's default is automated deletion no later than 30 days after the citation is resolved by payment or dismissal.

13. What happens to a potential violation that is rejected and never becomes a citation?

The policy states that the data will be destroyed within 30 days, or sooner when required by law.

14. Who can access program data?

Access is limited to authorized Altumint personnel and authorized personnel of its government safety partners. Access is based on job responsibilities and approved needs. Access is reviewed and removed when it is no longer required.

15. What security protections does Altumint use?

The policy states that violation images and data are encrypted at the time of capture and stored using recognized standards for securing legal evidence. It also describes role-based access controls, authentication requirements, training, screening, and access management.

16. Does Altumint use Social Security numbers in its traffic-enforcement program?

No. Social Security numbers are never used, linked to names, or printed on violation notices.

17. Does Altumint sell or monetize personal information?

No. Altumint will never sell, license, or otherwise monetize personal data collected through its traffic-safety program.

18. Does Altumint give other law-enforcement or federal agencies access to its program data?

Altumint does not proactively share, bulk-transfer, or provide standing access to program data to other law-enforcement or federal agencies. A request must be based on specific, individualized, legally valid compulsory process and must be escalated to Altumint Legal Counsel and the government safety partner before a response.

19. Can Altumint share data with service providers?

The policy permits sharing with authorized service providers working on behalf of Altumint or its government safety partners when needed for the program. It also permits disclosure when compelled by valid legal process, such as a specific warrant or court order.

20. What is SOC 2 Type II compliance?

SOC 2 is a widely recognized framework for evaluating controls related to areas such as security, availability, processing integrity, confidentiality, and privacy. Altumint's SOC 2 Type II compliance involves an independent CPA audit and must be maintained annually.

21. What is CJIS compliance and why does it matter?

The FBI's Criminal Justice Information Services Security Policy establishes security requirements for access to, storage of, transmission of, and destruction of Criminal Justice Information. Altumint's identifies requirements including multi-factor authentication, fingerprinting of authorized users with access to enforcement data, restricted access, and ongoing employee participation.

22. What is Altumint's relationship with Nlets?

Altumint is an Nlets strategic partner. Nlets partners undergo technical and financial vetting, a security audit before connectivity, and formal board or committee approval.

23. Does Altumint operate traffic-enforcement programs anywhere it wants?

No. Altumint says it will deploy a program only where state or local government has authorized the applicable automated traffic enforcement and where required regulatory approvals have been obtained. Camera locations, enforcement hours, and violation thresholds must also comply with that authorization.

24. How does Altumint check that it is following its privacy policy?

The policy identifies internal oversight and board monitoring, monthly data-destruction reporting, annual confirmations, SOC 2 compliance, Nlets participation, CJIS training, annual review of the privacy policy, internal audit review, public posting of the policy, and monthly client certification reporting.

25. What is the simplest way to understand Altumint's approach to privacy?

The policy describes a limited-purpose model: traffic-safety cameras are used for authorized traffic enforcement; non-violating vehicles do not create retained or transmitted records; program data is not used to track people or vehicles; photo enforcement is not integrated with ALPR, sound detection, facial recognition, or unrelated surveillance technology; access is restricted; and data is deleted according to defined retention rules.