

**CITY OF LOS ANGELES**  
INTER-DEPARTMENTAL MEMORANDUM

Date: December 15, 2025

To: The Honorable City Council  
c/o City Clerk, Room 395  
Attention: Heather Hutt, Chair, Transportation Committee

From: Laura Rubio-Cornejo, General Manager   
Department of Transportation

Subject: **PROTOCOLS TO SAFEGUARD THE PRIVACY OF INDIVIDUALS WHO RECEIVE CITATIONS**

**SUMMARY**

In response to Council File [13-0586](#), this report provides an overview of the Los Angeles Department of Transportation's (LADOT's) protocols and data retention policies that safeguard the privacy of motorists who receive a parking citation, and the privacy measures in place for future contracts with vendors.

**RECOMMENDATION**

That the City Council NOTE and FILE this report.

**BACKGROUND**

In June 2025, the City Council approved an amendment to LADOT's Parking Citation Processing Agreement (C-124676) with Modaxo Traffic Management USA, Inc. (Modaxo). As part of the approval, the Council instructed LADOT to report-back on existing protocols that safeguard the privacy of individuals who receive citations, including any data retention policies and regulations that prevent the long-term storage of data and personal information, and indicate how LADOT will implement these privacy measures across any new technology or future contracts with vendors.

**DISCUSSION**

Access to personally identifiable information (PII) in public records at state and local levels of government in Los Angeles is controlled primarily by the California Public Records Act (Government Code Section 6250, et seq.). However, the City of Los Angeles developed its own protocols in order to safeguard public privacy, while handling PII in accordance with applicable City policy and law, some of which is outlined in the Standard Conditions for City Contracts (Rev. 1/25 [V.2]) (Standard Provisions) that is appended to all City contracts. To take it one step further, in 2019, LADOT established its own data protection principles that apply to all data collected by operators and contractors responsible to carry out the City's and the Department's data protection responsibilities. These principles include:

1. **Data categorization:** Designate certain raw data as confidential information under the City's Information Technology Policy Committee Information Handling Guidelines. This long-standing policy for the City governs the obligations of the City to protect all manners of data under its control.

2. **Data minimization:** Collect only necessary data to meet specific operational and safety needs.
3. **Access limitation:** Limit access to what is required for operational and regulatory needs.
4. **Security:** Enact appropriate administrative, physical and technical safeguards to secure and protect data.
5. **Transparency for the public:** Publish certain information that does not contain PII with the public to increase transparency, accountability, and customer service and to empower companies, individuals, and non-profit organizations with the ability to harness a vast array of useful information to improve life in our city.

Consistent with the principles above, all LADOT record requests originating from a law enforcement agency for PII collected by the City require a subpoena and consultation with the City Attorney's office for appropriate processing to ensure compliance with City policies.

#### *Citation Processing Protocols*

For the purposes of parking citation processing, LADOT only collects PII from individuals who receive citations in order to process the violation in accordance with the California Vehicle Code. The contract between LADOT and Modaxo contains several provisions regarding the protection of PII and other confidential data, including compliance with Mayor Garcetti's Executive Directive No. 3, which establishes an "open data" policy in the interest of transparency, "subject to valid privacy, confidentiality, security, and other legal restrictions" regarding PII. Additionally, the contract includes instructions for storing and archiving data related to parking citation processing, securing data, and restricting access to data to only authorized personnel. For data stored on state-wide systems, the degree of security is higher and more restricted according to State of California law. All information obtained by the contractor pursuant to the contract is to be held confidential unless written permission by the City is provided.

In addition to the standards set forth by existing government regulations, LADOT and Modaxo utilize security measures, such as two-factor authentication and permission restriction, to ensure that PII is only accessible by authorized personnel. City systems utilize secure data networks, protected by industry-standard firewalls and password systems, with access restricted to trained, authorized personnel only. Encryption is employed especially when sensitive information is involved, and unique user IDs are assigned to provide an auditable record trail. Access to the citation processing system is strictly controlled and is only accessible through secure terminals.

#### *Data Retention Policy for Parking Citations*

The City's data retention policy for parking citations is a minimum of five years, which is included in the parking citation processing contract. Parking citations are archived on a quarterly basis by Modaxo on behalf of the City once the citation reaches the five-year mark. All data must also be backed up on a daily basis, with strict control and reconciliation procedures in place for system updates. Backups are performed every weekend and "duplexed," with one copy delivered to a secure offsite vault within 24 hours, while the other copy is kept at the contractor's data center. Daily incremental backups are also required for all non-database datasets.

### Other LADOT Programs with Privacy Protections

#### *Bus Lane Enforcement System (BLES)*

Assembly Bill (AB) 917 was signed into law in October 2021, authorizing public transit agencies statewide to implement programs that collect video images of parking violations in bus lanes and zones and partner with local jurisdictions to issue and adjudicate parking citations. As approved by the City Council ([CF 21-1224](#)), the bus lane enforcement program launched on November 1, 2024, with Los Angeles County Metropolitan Transportation Authority (Metro). Bus-mounted cameras identify vehicles parked in bus lanes and at bus stops, and submits the violation evidence packages to LADOT. LADOT confirms the validity of the violations, processes and issues the citations, and manages the administrative review and hearing process for contested citations.

This joint LADOT/Metro program adheres to more specific requirements in AB 917. The bill requires that video image evidence from forward-facing automated enforcement devices that does not contain evidence of a parking violation occurring in a transit-only traffic lane or at a transit stop shall be destroyed within 15 days after the information was first obtained. The video image evidence may be retained for up to six months from the date the information was first obtained, or 60 days after final disposition of the citation, whichever date is later, after which time the information shall be destroyed. Similar to the handling of parking citation records, only trained authorized personnel from the City and contractor(s) are allowed access to the systems where the video images and photographic evidence for bus lane violations are reviewed and processed. Once the bus lane violations are approved, a parking citation record is created for each incident and follows the data retention policy for parking citations.

#### *Automated Speed Enforcement (AB 645)*

In October 2023, Governor Newsom signed AB 645, which became law on January 1, 2024. The Bill authorizes the City of Los Angeles to install up to 125 Speed Safety Systems in order to calm traffic, reduce speeds, and reduce injury collisions. As of August 2025, LADOT onboarded a consultant to analyze locations for the installation of systems for this pilot, and draft the required Safe System Use Policy and Safe System Impact Report, as outlined in [CF 23-1168](#).

As required by AB 645, photographic evidence obtained from a speed safety system that does not result in the issuance of a notice of violation is required to be destroyed within five business days after the photograph was first made. The use of facial recognition technology in conjunction with a speed safety system is prohibited. Additionally, information collected can only be used to administer the program, and cannot be disclosed to any other persons, including, but not limited to, any other state or federal government agency or official for any other purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding.

Prior to implementation of the program, and as required by law, the City will adopt a use policy laying out these and any further restrictions on how data within the system can be utilized by the contractor, thereby further safeguarding the privacy of individuals receiving citations.

### Implementation Across Future Technologies and Contracts

LADOT's data protection principles resulted in the development of the Master Data License and Protection Agreement that adds strict administrative, technical, and organizational security measures to all future LADOT contracts that deal with PII. Key aspects of the Master Data License and Protection Agreement include:

- Security Measures: No less stringent than those applied to their own confidential data.
- Encryption: All City Data at rest and in transit must be encrypted with solutions certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent.
- Access Limitations: Precautions must be taken to prevent unauthorized access, protect data from loss or alteration, and prevent disclosure of credentials.
- Security Best Practices: The Contractor must implement least privilege, separation of duties, and role-based security.
- Credential Restrictions: Access to administrative credentials for City Data is restricted to essential personnel, with assigned usernames and passwords, encryption of credentials, and prompt revocation of access.
- Physical and Environmental Security: Facilities processing City Data must be secure with perimeter security.
- System Administration and Network Security: Operational controls, antivirus protection, vulnerability management, patching, and network security controls (firewalls, intrusion detection) are required.
- Logging and Monitoring: Networks and personnel must be continuously monitored for malicious activity, and logs of administrator activity and data recovery events must be maintained.
- Policies, Assessments, and Audits: The Contractor must have a formal information security program, perform annual vulnerability and risk assessments (including penetration tests), and allow City audits.
- Data Backup and Emergency Recovery: A multi-layered approach to backups and disaster recovery is required, including a primary and backup data center, semi-annual disaster recovery tests, and a written Disaster Recovery Plan.
- Data Return and Destruction: At the agreement's conclusion, City Data must be returned, deleted, or destroyed using industry best practices, with certification of destruction within 45 days.
- Data Breaches: The Contractor must notify the City of any Data Breach or Security Incident within 48 hours (or the next business day), begin immediate remediation, provide updates, and cooperate with investigations.
- Protection of Confidential Information: The Contractor shall not disclose any Confidential Information, shall limit access to Confidential Information, and shall protect Confidential Information from unauthorized use, access, or disclosure.

The new Parking Citation Processing Services contract with Modaxo conforms to the City's Master Data License and Protection Agreement and the City's Standard Provisions. The new contract adds more explicit data privacy protections in addition to or in lieu of what is provided for in the City's Standard Provisions. For example, the contract has a specific section dedicated to data protection that states the contractor will protect "consumer-provided data acquired in the course and scope" of the contract. The new contract expressly forbids Modaxo from "selling, leasing, distributing, publishing or otherwise sharing any personal information collected from customers, including, but not limited to, transaction history, address, email address, phone number, and credit card information." The contract also gives the

City explicit ownership “of all data and rights to the data” in the parking citation processing system, which shall be securely hosted by the contractor on its servers. At the termination of the contract, all data must be delivered to the City.

As emerging technologies are approved for use by the State of California, corresponding privacy regulations continue to evolve, becoming progressively more stringent in order to enhance and safeguard consumer privacy rights.

**FISCAL IMPACT STATEMENT**

There is no impact to the General Fund as this report is informational.

LRC:TC:KH:PR:dg/gd