

Los Angeles Department of Transportation

Automated License Plate Recognition Use Policy

Background

Automated License Plate Recognition (ALPR) is a technology that uses optical character recognition and image analysis to automatically capture, read, and process license plate information from vehicles. ALPR systems use cameras placed in strategic locations, such as on traffic signals, street lights, or parking facilities. ALPR cameras capture images of passing vehicles, extract the alphanumeric characters from their license plates, and convert them into machine-readable text. ALPR systems can be a valuable tool for enhancing public safety and facilitating automated processes for a variety of applications, including curbside parking management and parking enforcement.

The use of ALPR technology allows the Los Angeles Department of Transportation (LADOT) to collect comprehensive curb activity data to inform smarter policies and regulations; increase compliance with curb policies through automated payment and enforcement; and incentivize turnover and create easy access to curb space for drivers. Key outcomes of an effective ALPR program are reductions in greenhouse gas emissions, improved operational efficiencies, digital permitting, reduction in erroneous citations, seamless frictionless payments, and increased revenues. It is an important tool in LADOT's effort to implement a digital curb management program that reduces idling, better organizes the curb, reduces unsafe parking activities, and increases compliance with parking regulations.

This document summarizes how LADOT can implement ALPR to better organize the curb and increase roadway safety, how data and privacy will be protected, which outcomes are expected to be achieved, and how performance will be measured.

ALPR Policy

LADOT shall maintain administrative authority as well as processes and procedures regarding:

- General Compliance
- Administrator, Operator, Provider Requirements
- Systems Hardware and Operating Standards
- Data Collection, Storage, and Management
- Data Sharing and Public Information Requests
- Enforcement and Invoicing Administration
- System Oversight and Audit Procedures

Definitions and Acronyms

General Definitions

- “Authorized Users” means the LADOT staff and any Contractors who are granted authority to access an ALPR System for performing or assisting in carrying out an authorized use.
- “Automated License Plate Recognition Data,” or “ALPR Data” means information or data collected through the use of an ALPR System.
- “Automated License Plate Recognition System” or “ALPR System” means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.
- “Contractors” or “Contractor” means technology providers or other vendors who provide operational or support services for ALPR Systems in order to carry out an Authorized Use.

Data Type Definitions

- “Aggregated and Anonymized Data” means data that has been combined to communicate details only in terms of totals or summary and for which personally identifiable information has been removed, conforming to standards defined in NIST - 8053 and/or other City of Los Angeles policies that guide de-identifying data treatments.
- “Appended Data” means data added or supplemental to the Processed Data linked or otherwise joined through a machine or manual review process.
- “City Data” means any Raw Image Data, Processed Data, or Appended Data.
- “Derived Data” means data or information of any kind derived as a result (directly or indirectly) of upstream Raw Data, Processed Data or Appended Data data being compiled, aggregated, manipulated, modeled, analyzed, visualized, or other similar treatments for purposes of building insights and analysis.
- “Hit Event” means any ALPR Data or images downloaded to City servers that are associated with citations, infractions, or other pre-defined administration actions. Hit Events may comprise any or all of the other data types defined by this policy.
- “Raw Image Data” means unprocessed, non-annotated, point of collection image, point cloud, infrared or other data collected by ALPR cameras or associated sensors.
- “Read Data” means any Raw Image or Processed Data collected by the ALPR System that does not result in a Hit Event.
- “Processed Data” means data produced from raw images through a machine or manual review process.

Data and Information Designations Definitions

- “Confidential Information” means Raw Image and Hit Event Data collected by ALPR technology as well as Processed Data that appends any personally identifiable information to images and events.
- “Internal Information” means Derived Data products, insights, visualizations, forecasting models, and reports developed from aggregations and collections of raw images and events that are de-identified, aggregated, and that cannot be reverse engineered to identify individual persons or vehicles.
- “Restricted Information” means certain information specifically designated by LADOT to which the Department applies enhanced data protection measures, including, but not limited to those practices mentioned in the Information Technology Policy Committee (ITPC) Data Handling Guidelines, namely, encryption in transit, at rest, and in-use, multi-part authentication, and physical locked storage of “walking” assets where such data might be stored (e.g., USB drives).

Purpose

The City of Los Angeles utilizes ALPR technology to capture, analyze, and store digital license plate data and images to enable the rapid identification of vehicles and associated information in support of curb management and related parking operations and enforcement activities.

Curbside deliveries have increased dramatically in Los Angeles, like many other cities across the country. This is especially true for same-day and instant deliveries. Conventional curb users, including passenger vehicles, buses, taxis, and bikes are now competing with ride-hailing services, food delivery vehicles, and delivery trucks. This competition and jockeying at the curb exacerbates safety concerns and increased pollution and congestion. Before the pandemic, the World Economic Forum projected an estimated 36% increase in commercial vehicles on city streets by 2030. This is expected to lead to a 32% increase in emissions, 21% increase in congestion, and an additional 11 minutes of commute time per passenger per day. Since that prediction was made, commercial vehicle use has surged, with e-commerce growing 44% in 2020 alone.

The use of ALPR technology allows the City to use comprehensive curb activity data to inform smarter policies and regulations; increase compliance with curb policies through automated payment and enforcement; and incentivize turnover and create easy access to curb space for drivers.

Authorized Uses

LADOT will only use ALPR Technology to collect license plate and associated vehicle data within the public view and in areas in which there is not a reasonable expectation of privacy, and shall not be used to surveil, harass, intimidate, or discriminate against any individual or group. The LADOT will not use

ALPR Technology for the sole purpose of monitoring individual activities that are otherwise protected by the First Amendment to the United States Constitution.

Authorized Uses under this policy include:

Use	Description
Curbside Management	The collection of policies, procedures, and practices that enable the City to effectively allocate the use of its curbs and other high-demand areas associated with the curb, including payments for specially designated loading zones.
Speed Limit Enforcement	California Assembly Bill 645 authorized a five-year pilot program for automated speed safety cameras in six selected California cities, including Los Angeles
Red Light Enforcement	California Senate Bill 720 created a program for cities to utilize a red light camera system to support pedestrian safety measures
Mobility and Traffic Planning	The process of analyzing the current state of the City's mobility system in order to design for future mobility needs.
Transit (Bus) Only Lane and Bus Stop Enforcement	ALPR cameras that are located on buses and other public transit vehicles for parking enforcement.
On-and Off-Street Parking Enforcement	Mobile or fixed ALPR cameras used for on-and off-street parking enforcement.
Off-street Parking Lots and Garages	ALPR technology located at entry and exit points in City-owned parking facilities, including processing and fulfillment of payments for parking fees.

This policy is separate from any ALPR technology used by the Los Angeles Police Department (LAPD). The LAPD maintains its own policy for ALPR.

Authorized Users

Authorized Users with access to ALPR Data are limited to staff within LADOT with a specific operational need, as determined by the General Manager or the General Manager's designee. Authorized Users also include Contractors that aid LADOT in carrying out the Authorized Use. LADOT will maintain a list of all Authorized Users and the user's specific operational need.

General Compliance and Relationship to Existing City Policies

- Compliance with Relevant Federal, State, County, Local Laws
LADOT shall comply with all relevant federal, state, county, and local laws in the use and administration of ALPR Systems. To the extent this policy is in conflict with any federal, state, county, or local law, the statute or regulation shall take precedence and this policy shall be updated to comply or harmonize with the governing law.
- California Consumer Privacy Act (“CCPA”)
This ALPR Policy considers and conforms to established rules and procedures for the handling, storage, and incident response of Personal Information and Sensitive Personal Information as described by the [CCPA](#). Although CCPA does not broadly apply to nonprofit entities or government agencies, the City and LADOT may contract with private entities to fulfill specific administrative and operations requirements relating to ALPR technology use. As such, this policy offers provisions and guidance for handling treatment of personal data covered by CCPA in anticipation of contracting.
- California State Law related to Automated License Plate Recognition Systems
California Civil Code §§ [1798.90.5-1798.90.55](#), [1798.29](#), and [1798.82](#) require public agencies that deploy ALPR or access ALPR Data to post a privacy and usage policy online. The law further requires public agencies to include the following provisions in the ALPR policy:
 - The authorized purpose for using the ALPR System and collecting ALPR Data.
 - A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR System, or to collect ALPR Data. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.
 - A description of how the ALPR System will be monitored to ensure the security of the information and compliance with applicable privacy laws.
 - The purposes for, process for, and restrictions on, the sale, sharing, or transfer of ALPR Data to other persons.
 - The title of the official custodian, or owner, of the ALPR System responsible for implementing state law requirements.
 - A description of the reasonable measures that will be used to ensure the accuracy of ALPR Data and correct data errors.
 - The length of time ALPR Data will be retained, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR Data.

The law also prohibits public agencies from selling or sharing the information except to another public agency, and imposes security and other requirements on system operators and on users of data from ALPR Systems.

Data Retention Requirements

This ALPR Policy compiles with State data retention requirements including those required by [California Government Code 34090.7](#).

Data Breach Notice

Pertaining to incident handling for data breaches, this Policy considers and conforms to the requirements referenced by [California Civil Code sections 1798.29](#) and [1798.82](#), which requires immediate disclosure of any breach of the security of the system following discovery or notification of the breach in the security of the data to any impacted resident of California.

City of Los Angeles and LADOT Information Technology and Data Management Policies

This ALPR Policy has been developed with consideration of, and in alignment with, the existing and pending City and relevant department and agency principles and guidelines with respect to information technology (IT), data governance, data management, and privacy, including:

- City of Los Angeles Master Data License Protection Requirements
- City of Los Angeles Information Technology Policy Committee (ITPC) Handling Guidelines (Policy No. IT-017)
- Retention Time Periods from Division 12.3(b) of the City of Los Angeles Administrative Code
- Information Technology Agency Data-Sharing Working Group Guidelines (pending)
- Information Technology Agency Data Code of Ethics (pending)
- Information Technology Agency Data Lake and Data Dictionary Alignment (pending)
- City of Los Angeles Open Data Standards and Guidelines (Policy No. IT-009),
- Los Angeles Department of Transportation Data Privacy Policy
- Los Angeles Department of Transportation Data Protection Principles
- Los Angeles Department of Transportation Parking Privacy Policy
- Los Angeles Department of Transportation Guidelines for Data Handling from Mobility Service Providers

As these various intersecting policies are amended, this ALPR Policy will also be updated to reflect necessary changes and ensure synchronization as much as possible. The General Manager or the General Manager's designee will be responsible for surveying for changes and affecting recommended policy changes on a regular basis.

Authorized User Training Requirements

Pursuant to California Civil Code Section 1798.90.51 (b), all Authorized Users shall receive training prior to being provided access to ALPR System and data. A record of all completed trainings will be maintained by LADOT. Training shall include:

- Applicable federal and state law;
- Functionality of the equipment; and
- Safeguarding password information, access to the ALPR Systems, and ALPR Data, and the following types of procedures:
 - Administrative

- Physical
- Technical
- Operational

System Hardware, Location and Siting Criteria

LADOT applies administrative, operational, technical and physical safeguards to manage the system hardware and location settings of ALPR cameras.

Installation, Maintenance, and Support

LADOT will require regular maintenance, support, upgrades, calibration, and regular refreshes of the ALPR system to ensure that it functions properly.

Hardware Minimum Specification and Capabilities

- Asset Management - LADOT will maintain a prioritization or process for mounting cameras and sensing hardware . ALPR cameras will be sited according to established prioritization criteria for pole attachments. LADOT and its Contractors will maintain an inventory of all ALPR cameras and siting locations.
- Utility/Traffic Box Connections - In the instance that ALPR technologies would be connected to traffic/utility boxes there will be notice provided to the relevant City agency or responsible entity, as well as consideration for technical/operational maintenance, and requisite training provided to City administrators and staff or other entity personnel that maintain the traffic and utility boxes.
- Minimal Technical standards for procured ALPR cameras:
 - Minimum accuracy rates of 90 percent for traffic counts
 - Minimum resolution of 2560x1920 (5mp)
 - Shutter speeds will be adjusted according to the external environment (for example, in brighter conditions adjust the shutter speed to capture at 1/5000 of a second and for darker conditions the optimal shutter speed would be 0.75 to 1 second)
 - Maintained clear camera view free of obstructions
 - The camera should not exceed 45 degrees in the vertical or horizontal direction.
- Notice to other agencies - LADOT will make law enforcement and other relevant agencies (e.g., Bureau of Street Lighting) aware of all LADOT ALPR cameras that are affixed to the agency's property or asset, including the siting locations via geo-coordinates, the names/brands of hardware, and serial number of hardware.

Permissions and Restrictions relating to Camera Siting

ALPR cameras may be attached to a mobile vehicle or deployed at a fixed location. ALPR will not be used to intentionally capture images in private areas or areas where a reasonable expectation of privacy

exists, nor shall it be used to harass, intimidate or discriminate against any individual or group. Examples of restricted locations for fixed cameras may include healthcare facilities, religious institutions, and schools. However, in areas where the benefits of the ALPR technology outweigh the privacy concerns, ALPR Systems may be installed after LADOT conducts public education and collects feedback from potentially impacted stakeholders.

Data Collection

ALPR technology and related applications are intended to enable LADOT to collect the following key data points for purposes of curbside management and other authorized uses according to this Policy:

- License plate number and state
- Vehicle make and model
- Vehicle location
- Vehicle arrival, dwell and departure times
- Visible vehicle permits, registrations, and other demarcation
- Proximate vehicles
- Curb infrastructure and use
- Proximate traffic activity
- Traffic incidents

While Raw Image Data may contain other data points and information, LADOT and its Contractors will seek to reduce any personal identifying information collected, and will not intentionally process, enrich, or analyze the data sets to identify persons, businesses, or organizations other than for purposes of completing relevant curbside management enforcement and administration. Neither LADOT nor its Contractors may extract or use Raw Image Data for purposes other than those described by this Policy.

LADOT's and Contractor's siting criteria will take reasonable steps to position the hardware such that it reduces the collection of information beyond these target data, and minimizes collection of sensitive and/or personal identifying information.

Data Types and Ownership

ALPR technology and data solutions involve the collection of Raw Image Data and the appending of related vehicle and registered business and personal identifying information for purposes of applying various curbside management interventions - incentives, price-related enforcement, etc.

This policy establishes the following data types relating to ALPR:

- Raw Image Data
Raw Image Data is unprocessed, non-annotated, point of collection image, point cloud, infrared or other data collected by cameras and/or associated sensors to detect:
 - Presence of vehicles

- Vehicle license plate images
 - Vehicle images
 - Logo or other markings on vehicles
 - Location information (i.e., GPS coordinates)
 - Contextual data (e.g., location, buildings, block information)
 - Data and time of image capture
 - Other items or persons in field of view
- Processed Data

Processed Data is data produced from raw images through a machine or manual review, process, including:

 - Vehicle license plate number: optical character recognition or other image-recognition technique to determine the license plate characters
 - Vehicle license plate state
 - Recognition of other permit, plate
 - Inferred vehicle type and physical identification (e.g., make, model, year, color)
 - Inferred vehicle propulsion (e.g., internal combustion, electric vehicle, alternative fuel)
 - Event interpretation (e.g., parking, standing, double-parking, etc.)
 - Macro data relevant to the processing of the image
- Appended Data

Appended Data is data added or supplemental to the processed data linked or otherwise joined through a machine or manual review process, including:

 - Vehicle registration information
 - Owner name
 - Registered address
 - Registration status
 - Associated vehicle, owner information
 - Special designation or permit
 - Other vehicle specification information (e.g., year, propulsion information, weight, registered use (personal vs. business))
 - Event determination
 - Automated or manual administrative or enforcement determination
 - Other data that is added or appended to the collected Raw Image Data that relies on identifying information determined by Processed Data.
- Derived Data

Derived Data is data of any kind derived as a result (directly or indirectly) of the data being manipulated. This type of data includes counts, analyses, trends, insights and other information that rely on combined, compiled, visualized, geo-located, modeled, or other treatments of aggregated and de-identified Raw Image, Processed, and Appended Data.
- Ownership by Type

For purposes of this Policy, LADOT designates Raw Image, Processed, and Appended Data as "City Data". Accordingly, it shall establish its ownership and assignment of those data types

through contractual agreements with its Contractors. All City Data transmitted to, stored/held, and in-use by the Administrators or by LADOT's Contractors must be designated and classed according to ITPC Information Handling Guidelines (see Data Designation, Storage and Protection Requirements section below).

The ownership of Derived Data and Information produced through ALPR systems interfaces and applications or through offline means using aggregations, compiling, decompiling, joins, analyses, renderings of City Data and other combined data types may be assigned to LADOT or its Contractors, depending on the party who processes and/or creates those data and data sets. Through its contractual provisions with Contractors, LADOT will establish clear ownership and assignment of Derived Data.

Data Processing, Enrichment, and Analysis

LADOT and its Contractors can process, enrich, and analyze Raw Image, Processed, and Appended Data, yielding Derived Data that can be used *for any purpose consistent with the Authorized Uses*. This includes:

- De-identifying and aggregating Read and Hit data
- Adding or appending data from internal and external sources
- Comparing data sets for purposes of benchmarking or quality assurance , or conducting other general data quality assessments
- Rendering or transforming data into reports, visualizations, graphs, spatial maps, interactive and/or web-based displays, etc.

Automated processes used to treat and process/subprocess data can be applied so long as LADOT and its Contractors and Subcontractors certify its process to de-identify and prevent reverse engineering and/or de-compiling to identify individual's vehicles, individuals, or other personal identifying information.

Neither LADOT nor its Contractors shall treat or combine data in a way that would enable identifying individual and personal information (e.g., combining with other internal or external data sources that would reveal vehicle, individual, or other personal identifiable information (PII)).

Neither LADOT nor its Contractors shall compile or aggregate locations, events, patterns of movement, time stamps/dates, etc. or any Raw Image, Processed, or Derived Data at individual vehicle or person level that would enable LADOT to track history, surveil, or model/predict the movements of individual vehicles and/or persons. The sole exception is aggregation of enforcement or administrative action history data relevant to specific vehicles and registered individuals/organizations in-line with this Policy's retention policy, and may only be used for further or follow-up enforcement and administrative actions only.

Precision, Accuracy, and Quality Control

Curbside management involves enforcement and administration of curb use based on existing and eventual codified vehicle and access permissions restrictions, incentives, and pricing, as well as performing simulations, trend analysis, ongoing monitoring, and planning of curb use.

This management, therefore, relies on high efficacy of ALPR technology in terms of precision (image), data quality, and downstream image/data processing accuracy. LADOT will evaluate and seek Contractors that can demonstrate high rates of precision tied to image quality and image recognition, as well as accuracy in terms of high rates of data and action accuracy, especially relating to enforcement and administration actions. LADOT will seek precision rates above 95 percent and accuracy rates at 99 percent, though rates will be confirmed on an individual Contractor basis, and will be delineated through contractual provisions and established as Service Level Agreements (SLAs). Through these SLAs, LADOT and its Contractors will establish methods to audit and certify maintenance of established SLA levels on a regular basis. LADOT will formulate contractual agreements that include specific provisions for cost penalties for breaching established SLAs, and terminations for recurring breaches that are not addressed through a mutually agreed and confirmed corrective action plan. Additionally, LADOT may offer Contractors financial incentives in its contract for maintaining and/or exceeding established SLAs.

Data Retention Periods

LADOT will comply with data retention requirements of any applicable state law related to specific ALPR use cases. However, as a general matter, LADOT will archive, anonymize, or destroy data once it is no longer required or after the data retention period has been met.

- Retention of Hit Event
All ALPR Data and images downloaded to City servers that are associated with citations, infractions, or other pre-defined administration actions (i.e., “hits”) shall be retained for a minimum of two (2) years and maximum of five (5) years in accordance with [Division 12.3\(b\)](#), City of Los Angeles Administrative Code.
- Retention of Read Data
Only Derived and Aggregated, Anonymous Data and metadata will be retained for curb management purposes. All images and PII from “reads” will be automatically purged from the system after 48 hours. However, Contractors may retain random samples of Read Data to ensure quality control and refinement of data collection if so stated in the contractual agreement with LADOT.
- Retention of Restricted Information
All Restricted Information shall be retained for a maximum of 5 years or until the information is no longer required or useful to LADOT.

- Retention of Confidential Information
All ALPR Data and images downloaded to City servers or held by Contractors that contain Confidential Information, not related to a Hit Event, will be automatically purged from the system after 48 hours. This data may be anonymized and aggregated before purged.
- Retention of Internal Information and Open Data
There is no retention limitation for Internal or Open Data.
- Retention of Derived Data
Derived, aggregated, anonymized data used to identify trends, conflicts, and other traffic-related information may be retained for an unlimited time period.

Data Designation, Storage and Protection Requirements

ALPR Data will be treated and designated in alignment with LADOT's existing Data Protection Principles and Master Data License Protection Agreement, as well as with reference to the ITPC Information Handling Guidelines, especially with respect to designations:

- Restricted Information
Select ALPR events and Appended Data or other associated enforcement, administrative, or case data may flow to subsequent Public Safety inquiries, investigations, court proceedings, legal actions, or other matters where the loss or corruption of these data might substantially impact the City legally, financially, and/or reputationally. On a narrow basis, Administrators and Contractors may designate specific ALPR Data sets as "Restricted Information," and as such, apply enhanced data protection measures, including, but not limited to those practices mentioned in the ITPC Data Handling Guidelines, namely, encryption in transit, at rest, and in-use, multi-part authentication, and physical locked storage of "walking" assets where such data might be stored (e.g., USB drives).
- Confidential Information
Raw image and event data collected by ALPR technology as well as Processed Data that appends any PII to images and events shall be treated by LADOT and Contractors as "Confidential Information." Accordingly, LADOT and Contractors shall apply the following treatments and standards relating to Storage and Protection of information designated as such:
 - Contractor shall implement and maintain appropriate administrative, technical and organizational security measures in order to safeguard against unauthorized access, disclosure, or theft of City Data. These will be reasonable and appropriate as determined by the volume and sensitivity of Confidential Information held by LADOT and Contractor.
 - Contractor shall encrypt all Confidential Information at rest and in-transit, and apply industry standards or better, for tokenization, fraud-use protection, format-preserving encryption, and data encryption technology. Encryption should be certified per US

Federal Information and Processing Standard 140-2, Level 2, or equivalent or higher. Additionally, Contractor shall secure and protect all City Data from hacking, viruses, ransomware, and denial of service and related attacks.

Internal Information and Open Data

LADOT anticipates that ALPR Data will yield critical operational and planning insights and trends that the Department requires to conduct its business. Derived Data products, insights, visualizations, forecasting models, reports developed from aggregations and collections of raw images and events that are de-identified, aggregated, and that cannot be reverse engineered to identify individual persons or vehicles will be treated as Internal Information or Open Data, depending on the status of the work product (draft, final, etc.), and based on review and approval by administrators. Based on these designations, LADOT and its Contractors will apply storage and protection measures commensurate with these designations, as defined by the referenced ITPC Data Handling Guidelines. Administrators and Contractors will also treat these designated data sets and related work products with the stipulated data minimization practices, as described in [LADOT Data Protection Principles](#): *aggregation, obfuscation, de-identification, and destruction*.

Other Storage and Provisions

Storage of any City Data “at rest”, whether on proprietary/dedicated servers or via cloud storage services, must be on servers or in data centers located in the continental United States of America. Any City Data stored on portable devices or electronic media, including personal computers, removable/portable data drives must be registered, encrypted, and the devices must be password-only accessible by Authorized Users, and those devices must not be removed from continental United States of America, unless that device is approved, is trackable via administrative controls, and includes remote wiping capabilities if the device is lost, stolen, or misplaced.

Confidential and Restricted Information can only be accessed for purposes of LADOT’s and Contractors’ business activities and processes directly related to Authorized Uses.

Data Disposal

Upon the termination of data retention periods applied to each data set, the City and its Contractors will dispose of retained data according to industry best practices for destroying electronic and hardcopy data sets.

- [City Data Disposal Process](#)

Administrators will dispose of any and all retained data in databases, hard-drive files, collaborative workspaces, on-premise data storage, cloud environments, and other relevant data repositories. All computer desktops, laptops, hard drives, and portable media must be processed

through the Department's dedicated data destruction process for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the Department's archiving and destruction policy that specifies a process for making sensitive information unusable and inaccessible, in such a way that data recovery using common techniques or analysis is greatly reduced or prevented. These procedures should specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed. Acceptable methods include, but are not limited to: shredding or incinerating physical media; overwriting, degaussing, or physically destroying electronic media. IT documentation, hardware, and storage that have been used to process, store, or transmit Restricted Information or Confidential Information shall not be released to the general public until it has been sanitized and all stored information has been cleared using one of the above methods.

As needed, LADOT will maintain an electronic log of data disposition and destruction to be available for audit. This can include event logs re: database actions, data disposition or manually curated logs.

- Contractor Data Disposal Process

LADOT Contractors that are handling ALPR Data of any type will be subject to data disposal and destruction procedures that are agreed through contractual provisions, and will be aligned to industry best practices. Contractors must submit Data Disposal process descriptions as Exhibits to their contractual agreements, and will maintain automated or electronic logs of contractor data disposals that describe both automated and manual destruction events, appropriate to the volume and sensitivity of the data, and in-line with the prescribed retention periods.

- Internal Information and Open Data Designated Data Sets: Aggregated/Derived Data Products

Unless explicitly required, Internal Information and Open Data shall not be disposed of, unless in the practice of the Department's IT policy or at the discretion of the LADOT or its Contractors.

- Enforcement and Administrative Data Disposal

LADOT and its Contractors will ensure that essential Enforcement and Administrative data required for minimum retention periods are protected from and NOT subject to disposal procedures. These specific event data and associated/appended information will be maintained by designated parties in specific areas so that relevant data objects and attributes can be disposed of in their native data sets, but are otherwise retained, as needed.

- Schedule of Data Disposals by Type of Data

Data Type	Retention Period
Hit Event	Minimum of 2 years; Maximum 5 years or until data is no longer needed for litigation purposes
Read Data	Maximum 48 hours
Restricted Information	A maximum of 5 years
Confidential Information	Unless considered "Hit Data," a maximum of 48 hours
Internal and Open Data	No retention period
Aggregated and Anonymized Data	No retention period

- Notification, Verification and Audit of Disposals

Through its contractual agreements, LADOT shall establish provisions to ensure that its contractors dispose of data according to and in-line with its permissible retention periods based on data type. Contractors should provide notice to LADOT upon scheduled disposals, and LADOT will maintain rights to independently verify disposals, and also audit the history of disposals to ensure that they are completed according to schedule.

Stored Data Access Controls

- System Access Controls

The following are preventive mechanisms that LADOT will use to ensure that the ALPR Systems are efficiently running and the data is secured:

- *Administrative:* Username and password-protected access to the ALPR System.
- *Operational:* Training system users on proper use and secure practices when using ALPR and its database.
- *Physical:* All network equipment and servers containing sensitive data are maintained in a secure off-site location, and accessed only by authorized personnel. This includes the secure storage of computers with access to the offsite database. ALPR Systems will require a multi factor secured virtual private network access to databases.
- *Technical:* All information is encrypted to protect any personally identifiable information. ALPR System workstations and servers shall be updated with the latest security patches on a regular basis. ALPR Data shall be secured, encrypted, and backed up regularly.

LADOT will establish operational procedures and controls for protecting Authorized User credentials and system access in accordance with internal standards or industry standard safeguards, such as:

- ISO/IEC 27002:2005,
 - NIST 800-44,
 - Microsoft Security Hardening Guidelines,
 - OWASP Guide to Building Secure Web Applications,
 - SOC 2 Type 2, and the various Center for Internet Security Standards.
- Password Management
LADOT will apply encryption to all passwords, passphrases, and PAINs, based on US Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard.
- User Offboarding Procedures
LADOT will change passwords and/or restrict access immediately after an Authorized User ceases employment with the Department or is reassigned to a role that no longer requires user access.
- Monitoring and Reporting Abnormal Usage (log-in, access, and data transfer events)
LADOT or the ALPR System will maintain a log of successful and unsuccessful login attempts, with such logs monitored by the Department's Authorized Users. LADOT will update ALPR System workstations and servers with the latest security patches on a regular basis.

Customer Data Privacy

For customers who register with external system interfaces and submit their personal information and sensitive personal information (e.g., PII, financial, credit, bank account information, etc.) in order to enable payments and settlements relating to workflows associated with various ALPR uses, this Policy requires that those data be handled in accordance with and as required by CCPA. This handling will extend to any third parties or contractors that manage associated technology platforms, payment systems, enforcement workflows.

Privacy policies and practices, in addition to this Policy, will be posted publicly on websites that are tied to uses of such systems and will also be available within the technology applications themselves, so that customers have immediate access to information relating to how their information and PII is being secured and used.

Enforcement and Invoicing Administration

ALPR technology enables LADOT to automatically notify and/or invoice drivers for the exact amount of time spent at the curb, eliminate/reduce the need for physical meters and location-based mobile applications, and make it easier for commercial fleets to pay metered rates for stops at the curb for loading and unloading.

Additionally, ALPR technology enables LADOT to automatically capture parking violations and parallel violations like double-parking in real-time. Using the ALPR technology, LADOT can send citations automatically by mail to the registered owner of the vehicle or direct parking enforcement officers to the infraction location in real-time. LADOT may rely on Contractors and Subcontractors to perform enforcement or administrative services and follow-up actions.

To the extent authorized by state law, LADOT may utilize ALPR to notify and invoice drivers for time spent at the curb and to issue citations for parking related violations by mail to designate the mailing address of the subject's vehicle's registered owner, or through e-mail or web-application processes.

LADOT will review its Enforcement and Administration accuracy rate at which it or its Contractor performs, as well as rates of "false positives" and "false negatives". LADOT seeks a 100 percent accuracy rate, and will record all cases of inaccuracy, and designate root cause for "false positives", especially. For high rates of or recurring root causes for false positives, LADOT and its Contractors will develop a corrective action plan in attempts to address root causes.

Incident, Data Breach, Notification, and Incident Response

Incident:

- Accidental exposure/sharing of Confidential or Restricted Information to unauthorized parties
- Loss or damage of Confidential or Restricted Information or media holding data with these designations
- Discovery of improper or negligent data storage practices
- Improper disposal practices
- Other forms of data breach

LADOT shall maintain a written log of all incidents. The ALPR System Oversight Manager shall review each incident relating to the volume and sensitivity of data involved and determine appropriate notifications, as needed.

Specifically following the discovery of a breach of the ALPR System that results in unauthorized third party disclosure of Restricted or Confidential Information containing PII, LADOT shall disclose the breach to all impacted individuals as required and in accordance with the threshold required by local, federal and state laws (especially CCPA), in the most expedient time possible and without reasonable delay, by providing a notification to those reasonably believed to have been affected by the breach, and include the following:

1. "Notification of Data Breach"
2. "What Happened"
3. "What Data Was Involved"
4. "What We Are Doing"
5. "What You Can Do"

6. "For More Information"
 - a. Name and contact information for department reporting the breach
 - b. A list of the personal information subject to the breach
 - c. Either the date, estimated date, or the date range that the breach occurred if the information can be determined when the notice is provided
 - i. If notification was delayed as a result of law enforcement investigation
 - ii. A general description of the breach incident

Data Sharing and Compliance with Court Orders and Legal Processes

LADOT does not share Raw Image Data with any commercial or private entity, other than its Contractors, only as necessary to conduct City parking operations. LADOT includes confidentiality provisions in its agreements with any parking contractors and/or vendors to prohibit any use or distribution of Raw Image Data for any purpose other than the Authorized Uses under this Policy. Data gathered or collected and records retained by LADOT must not be: sold, published, exchanged, or disclosed for commercial purposes.

LADOT and curb management contractors may share, distribute, and/or release for public consumption or for commercial uses Aggregated and Anonymized Data in order to increase transparency, accountability, and customer service and to empower companies, individuals, and nonprofit organizations with the ability to harness a vast array of useful information to improve life in LA. LADOT will not release any ALPR Data until data de-identification and destruction treatments are implemented.

Law enforcement and other government agencies, whether local, state, or federal will not have access to Raw Image, Processed, or Appended Data other than as required by law, such as a court order, subpoena, or other legal process. To be clear, LADOT will make no data available to law enforcement agencies through this process that is not already available to them. *See also:* [LADOT Data Protection Principles](#)

Public Information Rights/Handling of California Public Records Act (CPRA)

Public Information includes any data compiled or maintained by a city government. Under California law, city departments are required to disclose government records to the public upon request, unless exempted by statute CPRA California Government Code 6250 through 6276.48).

Dissemination of Public Information does not require specific approval from the owner. Public Information can be viewed or copied without restriction. The decision to make a piece of information available to the public should be deliberate and approved according to the Open Data Policy and the CPRA.

All Public Information requests will be reviewed by the designated ALPR System Administrator for consideration; as needed, select requests will be submitted to and reviewed by the City Attorney.