

# **The Los Angeles County Sheriff's Department's Automated License Plate Recognition (ALPR) Privacy Policy**

The purpose of this privacy policy is to ensure that all conduct of the Los Angeles County Sheriff's Department (Department) and its personnel related to the capture, use, retention, and dissemination of information obtained through the use of the Automated License Plate Recognition (ALPR) System complies with all applicable federal, state, and local laws.

ALPR technology is a valuable tool for law enforcement and when used appropriately serves to enhance public safety. As with any law enforcement capability, the technology must be used in a manner that is consistent with the United States Constitution, including the Fourth Amendment, and other applicable statutory authorities.

The Department acknowledges and fully intends to comply with the array of statutes, regulations, and policies that guide law enforcement on how it may and may not collect, retain, and disclose data, as well as requirements regarding notification in the event of a data breach.

## **I. Authorized Purposes for Use of ALPR Technology**

The Department intends to the use ALPR technology for the following public safety purposes:

- Investigation for prosecution or exoneration of suspected criminal (including terrorist) incidents.
- Identification and/or location of wanted persons.
- Enforcement of sanctions, orders, or sentences.
- Crime prevention/general law enforcement purposes.
- Crime analysis.
- Investigatory leads in subsequent investigations.

## **II. Persons Authorized to Use or Access ALPR Technology/Data**

Designated personnel appropriately trained on use of ALPR may gather data using ALPR technology.

Information collected via ALPR technology will be analyzed only by qualified individuals who have successfully completed a background check, have appropriate security clearance and have been approved and trained accordingly.

Sworn personnel or authorized civilian personnel (role-based such as crime analyst) will have general user access to the LASD ALPR database, as appropriate, to query information.

Sworn personnel or authorized civilian personnel (role-based) of the Advanced Surveillance and Protection Unit (ASAP) or Sheriff's Data Network (SDN) Unit will have administrative user access to the LASD ALPR database, as appropriate, to control:

- The information to which a particular group or class of users can have access based on the group or class.
- The information a class of users can access, including specific sites and/or data being utilized in specific investigations.
- Sharing capabilities with other law enforcement agencies.
- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the data or equipment.

### **III. Guidelines Regarding Appropriate Use**

ALPR data must be collected in a fair and lawful manner in the routine duties of law enforcement.

LASD will not seek or retain information about individuals or organizations solely on the basis of religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

Department members shall use information-gathering and investigative techniques that are the least intrusive means necessary in the particular circumstances to gather information the Department is authorized to seek and/or retain.

Data shall only be accessed for appropriate, job-related functions. Data shall not be used for any non-work-related purpose, and all uses shall take into consideration the privacy, civil rights, and civil liberties of individuals.

### **IV. Quality Assurance**

The Department will investigate in a timely manner alleged errors and deficiencies (or will refer them to the originating agency) in order to correct, or refrain from using protected information found to be erroneous or deficient. Original data will not be altered, changed, or modified in order to protect the integrity of the data.

LASD will make every reasonable effort to ensure that information retained is derived from dependable and trustworthy sources which convey accurate, current, and complete information, including the relevant context in which the information was sought or received.

The labeling of retained information (hotlist Information) will be evaluated by LASD or the originating agency when new information is gathered that may impact the reliability (content validity / software misread) of previously retained information.

LASD will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information from the ALPR System is correct.

### **V. Sharing and Disclosure**

LASD does not share ALPR data with any contracted, commercial, or private entity.

The provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information (see CA Civil Code 1798.90.55.(b)).

Information gathered or collected and records retained by LASD may be accessed or disseminated for legitimate law enforcement, criminal justice, or public safety purposes only to persons or entities authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who accessed information, and/or received information retained by LASD; the nature of the information requested and/or accessed, and the specific purpose will be retained by LASD for a minimum of two (2) years.

Information gathered or collected and records retained by LASD will not be:

- Sold, published, exchanged, or disclosed for commercial purposes.
- Disclosed or published without authorization.
- Disseminated to persons not authorized to access or use the information.

LASD shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

LASD shares ALPR data with other law enforcement agencies upon the execution of an inter-agency agreement by which each agency agrees that all ALPR data will be gathered, accessed, utilized, and disclosed in accordance with applicable law, and further agrees:

- ALPR data shall be available only to authorized users for legitimate law enforcement purposes.
- Reasonable efforts will be made to ensure the accuracy of its data.
- Shared hotlist data will not be stored for more than 24 hours without refresh.
- Internal audits will be conducted periodically to ensure information is up to date and user queries are made for legitimate law enforcement purposes only.
- Audit trails shall be maintained by each agency as defined by their policy.

## **VI. Information Retention and Destruction**

ALPR data will be maintained in accordance with applicable laws and County / Department retention policies. Data associated with a specific investigation or prosecution will be retained until final disposition of the case, or until the data has no further value.

Information will be reviewed for record retention (validation or purge) at five (5) years, and when information has no further value or meets the criteria for removal by applicable law, it will be purged or permanently deleted except in cases such as:

- ALPR records related to a prosecution will be maintained until a final disposition has been reached in the case.
- ALPR records can be maintained in the criminal case file and retained for the maximum period of time associated with such record.

- ALPR records associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.
- Whenever otherwise directed by an executive of the Department for a particular case or internal investigation.

LASD retains the right to remove ALPR data earlier, based on limitations of data storage requirements and other limitations including privacy concerns.

## **VII. Accountability**

All personnel authorized to use or access ALPR technology or data will be accountable for knowledge of this policy.

Department members shall report errors and suspected or confirmed violations of Department policies relating to protected information to their supervisor or manager.

All access to the system will be logged, and the Department will maintain an audit trail of requested and accessed information, including the purpose of the query. Periodic, random audits will be conducted to ensure and evaluate compliance with system requirements and with the provisions of this policy and applicable law. Audit trails will be maintained by LASD for a minimum of two (2) years.

LASD will annually conduct an inspection of the audit information contained in its database system(s). The inspection will be conducted by the ASAP Unit. The ASAP Unit has the option of conducting random inspections, without announcement, at any time and without prior notice. The inspection will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Department's information system(s).

## **VIII. Custodian of ALPR System and Records**

Primary responsibility for the maintenance and operation of the ALPR database and coordination of personnel and agencies receiving, seeking, and evaluating the information as well as quality, analysis, destruction, sharing, disclosure, or dissemination of further information will be assigned to the Advanced Surveillance and Protection Unit (ASAP). The ASAP Unit will serve as the Department's custodian of records for the ALPR System and data.

## **IX. Training**

Field Operations Directive 09-004 (FOD) provides guidelines and procedures on the usage of ALPR equipment and has been provided and briefed to training staff at all stations regarding ALPR equipment usage and access. All personnel authorized to use or access ALPR technology have been provided with all relevant policies, directives, and procedures related thereto and are accountable for knowledge thereof.

There are formal training classes on the authorized search engines which access and query ALPR data. Training is also conducted by station training personnel and the ASAP Unit. The basic ALPR software interface is intuitive and specific queries can only be done after all the information is collected, including search purposes and identifying information as to the individual conducting the search. There are also detailed help tutorials within the basic ALPR software to assist with helping each user to run certain basic queries.