GEORGE GASCÓN
District Attorney

Automated License Plate Recognition (ALPR) Policy

The San Francisco District Attorney's Office (SFDA), the chief law enforcement agency for the City & County of San Francisco, investigates and prosecutes crime in San Francisco and supports victims of crime. The Office works tirelessly to hold offenders accountable and protect victims, and innovates to break the cycle of crime.

Authorized Purpose for Accessing and Using ALPR Information

The San Francisco District Attorney's Office (SFDA) is an automated license plate recognition (ALPR) end-user, which accesses license plate information from systems controlled by ALPR operator agencies to investigate and prosecute criminal activity in the City & County of San Francisco. SFDA uses ALPR information to identify vehicles associated with criminal targets.

Authorized Users of ALPR Information

The following SFDA staff involved in the investigation and prosecution of crime are authorized to access and use ALPR information:

- District Attorney
- Assistant District Attorneys
- District Attorney Investigators
- District Attorney Analysts
- District Attorney Paralegals

Training

SFDA provides an annual staff training on the secure handling of confidential and personal information, including ALPR data. The training addresses appropriate handling and transmission procedures, as well as consequences of a security breach.

ALPR Information Security

ALPR information that is being used in SFDA investigations and/or prosecutions is stored on a securely as follows:

- Physical Security - All network equipment and servers that contain sensitive data are kept in a secured location and only accessible by authorized personnel.
- Access Control - To prevent unauthorized access of data, each security group is assigned least access and users are added to those groups.
- Encryption - SFDA's network is protected behind the City's firewall and data transmitted outside the SFDA's network to our cloud based partners are encrypted via SSL/TLS. Data at rest offsite are also encrypted.

- Monitoring - All of SFDA's servers and Network equipment are monitored 24/7
- Logging - successful and unsuccessful logon attempts, changes on user account, modify logs, network threats and resource access are logged.
- Patch management - All SFDA's workstations and servers are patched regularly.
- Backup - All sensitive data stored on the servers are backed up regularly and a copy saved offsite for DR. Data saved offsite are encrypted.

If necessitated by law enforcement or public safety purposes, SFDA shares ALPR information via the San Francisco City & County email server and/or One Drive which is CJIS certified. Any time the information is shared, recipients are instructed that the information they are receiving contains confidential information protected by law, which may not be further disseminated.

Microsoft Azure, Exchange Online, SharePoint and OneDrive are certified for CJIS compliance. A copy of O365 Security document can be found here: Security in Office 365

SFDA adheres to all applicable privacy laws.

Audit

SFDA conducts an annual audit of all investigations and prosecutions for which ALPR information has been accessed, documenting the number of pending and closed cases for which ALPR data has been retained, as well as the number of records for which ALPR data will be deleted pursuant to the SFDA data retention policy (see below).

When requesting ALPR information from the ALPR operator, SFDA is required to submit a case number (either the investigation case number, incident report number or court number, depending on the stage of investigation/prosecution). This case number is attached to all files that include ALPR information.

Audit results are shared with the official SFDA custodian for implementing the ALPR policy.

ALPR Information Sharing Restrictions

SFDA only shares ALPR information with authorized law enforcement partners for public safety purposes. SFDA does not share this information with commercial or other private entities or individuals.

Official Custodian

The Managing Attorney of the SFDA Crime Strategies Unit is the custodian for implementing the SFDA ALPR policy.

Accuracy of ALPR Information

In the event that an ALPR operator informs SFDA of an error associated with ALPR information accessed by SFDA, SFDA will correct all associated files.

Should SFDA become aware of an ALPR error, it will correct all associated files and contact the operator that provided the information regarding the error.

ALPR Data Retention

In accordance with the SFDA Record Retention and Destruction Policy, ALPR data will be stored as per the following schedule:

- Investigation File: 2 years
- Misdemeanor Discharge: 2 years
- Misdemeanor Court Case: 2 years
- Felony Discharge: 7 years
- Felony Court Case: 50 years
- Homicide Record: Permanent

*Data retention is based on departmental needs.