FAQ

Managing your LPR data

Frequently asked questions

Motorola Solutions hosted environment presents a great convenience to customers wishing to deploy license plate recognition (LPR) in a scalable fashion without concern of servers, storage space, database maintenance or software updates. Using a hosted environment benefits agencies in many ways, but it does present some questions for those not familiar with hosting data in the cloud.

Q. How does data sharing work?

A. Motorola Solutions maintains three distinct license plate recognition (LPR) platforms, VehicleManager, VehicleManager Enterprise and ClientPortal. All data collected by Motorola's customers, whether in VehicleManager, VehicleManager Enterprise or ClientPortal, is the property of the respective customer, and Motorola has no rights or ownership to any of this data. All customers manage and control all access to their LPR data as well as maintain their own data retention period, even on shared data.

VehicleManager is a hosted solution made available exclusively to law enforcement (LE) customers. The VehicleManager software and database, the data center housing VehicleManager, and the people and processes governing VehicleManager are compliant with all relevant aspects of the FBI-CJIS Security Policy. Law enforcement agencies may choose (at their sole discretion) to share their data to other law enforcement agencies within the VehicleManager platform, but there is no mechanism to share this data outside of VehicleManager.

VehicleManager Enterprise and **ClientPortal** are hosted solutions, similar to VehicleManager, made available to all enterprise customers. These customers consist of parking enforcement entities, parking management companies, property management and retail facilities, homeowners associations, casinos and many other types of enterprises.

As with law enforcement agencies in VehicleManager, VehicleManager Enterprise and ClientPortal customers may choose to share (at their sole discretion) their data to other VehicleManager Enterprise and ClientPortal customers. Unlike VehicleManager however, they also have the ability to share their data to law enforcement customers via a one-way sharing mechanism from VehicleManager Enterprise and ClientPortal to VehicleManager. To prevent the inadvertent sharing of data from law enforcement accounts, Motorola has physically separated Law Enforcement data within Azure Gov and enterprise data in Azure Commercial. This physical segmentation of networks blocks the data passing from VehicleManager (LE) data into our enterprise environments.

Q. What is "commercial data"?

A. We maintain a separate database of commercial LPR data. This data is collected by repossession vehicles. This data is not commingled with law enforcement or enterprise data, nor is law enforcement or enterprise data ever accessible to commercial entities. This is part of meeting CJIS compliance requirements for data access for our law enforcement customers. We provide our law enforcement and enterprise customers access to this commercial dataset to generate improved vehicle location insights with a greater quantity of data points.

Q. How long is my data stored?

A. As the data is your property, it is held according to the retention policy set forth by you. Retention policies may be adjusted by the Agency or Site Manager at any time, and different retention policies may be set for "detections" and "hits" to allow for consistency with any policy in place and/or legislation. Even if you choose to share data with specific law enforcement agencies, the data retention policies set on your data by you, still apply. Data is automatically deleted from the system based on the retention policy, and Motorola Solutions keeps no record of data after deletion unless metadata archival and classification is requested by the agency.

Q. How secure is my data?

A. Your data resides in a data center featuring redundant power sources, redundant fiber connectivity, redundant disk arrays, environmental monitoring, secure access control, physical escorts for on-site visitors, multiple diesel fuel backup generators, active fire prevention and suppression, and on-site system administrators and engineers. For our law enforcement customers, our systems are completely CJIS compliant, not only compliant because they are "Hosted in a CJIS Compliant Cloud." To meet CJIS compliance vendors must address:

- Data encryption from the edge to the cloud.
- Data can only be accessed by approved personnel.
- Data access is restricted, including to the vendor, and is totally managed by the agency.
- Criminal background checks of vendor personnel that have access to the data.
- Physical security safeguards at data center and critical infrastructure locations.
- Robust audits and accountability based on users, search parameters etc.
- System IP address logging for accountability of access.
- Multi-factor authentication for access to the data that can be coupled with optional secure single sign-on.
- Mandatory user logout after inactivity.
- Configured and managed user accounts to restrict or limit access based on roles.
- Printable audit reports for record management and challenges.

Additional safeguards

Built-in scheduled health and maintenance checks of systems and cameras.

- Report on every system and every camera.- Mobile health reports can report on your parameters – weekly, monthly, etc.
- Maintain easy accountability and proper use.
- Data retention is managed by the agency and can apply a custom required policy on both detections and open cases.
- Full auditing capability, including ANY users from a shared agency querying the data.
- Digital evidentiary data can be easily preserved for court (not a copy, but the raw data).
- Required reasoning notation to query the LPR database is mandatory.

See the full security briefing and compliance guide here.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com