



West Saint Paul Police Department 2017 ALPR Audit

Executive Summary

October 9, 2017

Background:

The West Saint Paul Police Department retained the services of a LOGIS Security Specialist, in order to audit the Agency's use of their ALPR system against the requirements of MN Statute 13.824. The West Saint Paul Police Department has an ALPR system on 2 squad cars and does not have any stationary ALPR units.

Department Policy & Procedures (MN Statute 13.824):

The West Saint Paul Police Department has an adopted ALPR Policy and has been keeping it updated to reflect the most current version of MN Statute 13.824. A review of this policy found that West Saint Paul Police Department was compliant in this part of the Statute.

Data Security (MN Statute 13.824):

The West Saint Paul Police Department's ALPR system is protected by Access Control users and groups that protects and controls access to the ALPR Data on a permitted basis only. User accounts and role based accounts are reviewed on a regular basis by ALPR administrators. West Saint Paul Police Department was found to be compliant in this part of the Statute.



Record Retention (MN Statute 13.824):

The West Saint Paul Police Department's ALPR backend BOSS system was audited to ensure each device setting was set for a retention period of no more than 60 days. West Saint Paul Police Department was found to be compliant in this part of the Statute.

Data Classification (MN Statute 13.824):

The West Saint Paul Police Department's ALPR Data that has been collected is classified as private data unless access to it is permitted by law. The ALPR system is on premise and the collected data is not stored in a state depository. Public data request of data collected on a license plate owner's vehicle is readily available through a proper records request through the West Saint Paul Police Department Records Clerk. West Saint Paul Police Department was found to be compliant in this part of the Statute.

Sharing Among Law Enforcement Agencies (MN Statute 13.824):

Appropriate sharing of ALPR data is conducted through inter agency requests. The requests are logged and reviewed by agency administrators. ALPR data requests to the West Saint Paul Police Department are compliant with 13.824. West Saint Paul was found to be compliant in this part of the Statute.

Public Log of Use (MN Statute 13.824):

The West Saint Paul Police Department ALPR admins, compile monthly reports that comply with 13.824 Subd. 5. These public logs are readily available through a proper records request. West Saint Paul was found to be compliant in this part of the Statute.

Notification to Bureau of Criminal Apprehension (MN Statute 13.824):

The West Saint Paul Police Department has made the required notification to the Bureau of Criminal Apprehension. This was validated on the BCA website. West Saint Paul Police Department was found to be compliant in this part of the Statute.



Biennial Public Accountability Audit (MN Statute 13.824):

West Saint Paul Police Department signed an ALPR audit agreement in May or 2017. Agency administrator understood the intent of the public accountability and provided easy access to policies and procedures, staff interviews and audit of the ALPR Systems. The Chief of Police acknowledge their intent to comply with MN Statute 13.824 and to continue audits every two years. West Saint Paul Police Department was found to be compliant in this part of the Statute.

Conclusion:

Based on the results of the West Saint Paul Police Department's ALPR Audit, LOGIS is able to confirm they are using the ALPR System as an effective law enforcement tool to help combat auto theft and other crimes linked to a vehicle license plates, and that their security and administration of the program is in compliance with MN Statute 13.824. Furthermore, as per statute, the West Saint Paul police chief has requested LOGIS to forward the results of this audit to:

The Minnesota Commissioner of Administration
The Legislative Commission on Data Practices and Personal Data Privacy
The Chairs of Legislative Committees

This Audit was conducted and attested to by:



Dimitrios Hilton

LOGIS Security Specialist

