# Washington SB 6002: What It Means for Agencies

In practice, SB 6002 affects several core parts of an agency's ALPR program:

### Access and sharing controls

Agencies must ensure ALPR data is available only to authorized users and that any sharing of data is intentional, controlled, and consistent with the law. This requires a review of user permissions, administrative access, and any interagency or external sharing workflows.

### Retention and recordkeeping

The law makes retention settings and recordkeeping practices a compliance issue. Agencies must know how long ALPR data is retained, how audit records are preserved, and how those records can be retrieved for audit, review, or disclosure. SB 6002 requires agencies to maintain audit trail data showing how the ALPR system is accessed and used. Agencies need records showing who ran searches, when those searches occurred, what information was queried, and what actions were taken in the system.

### Annual reporting

The bill requires agencies to prepare and publish annual reporting on ALPR usage, including activity levels, sharing activity, audit-related information, and camera locations. Agencies need a repeatable process for gathering and validating this information.

### Deployment review

Section 3(4) affects where ALPR systems can operate and requires agencies to review current deployment practices, especially for mobile ALPR workflows.

### Internal policy and workflow alignment

Because the law touches access, retention, sharing, auditing, and reporting, agencies need coordinated workflows across command staff, legal, records, and system administrators. ALPR programs that have been managed informally now require a more structured compliance process.

## What Agencies Should Do Now

Agencies using ALPR in Washington should review:

- who has access to ALPR data
- how sharing is configured
- how long ALPR data and audit records are retained
- whether audit logs capture the information needed for internal review
- how annual reporting will be compiled and published

## How Axon Software Can Support These Workflows

Axon software helps agencies implement these requirements through configurable access controls, sharing settings, retention controls, audit records, and reporting-related system data. The sections below explain how those capabilities map to specific provisions of SB 6002.

### Section 3(4): Restrictions on collection near certain locations

Section 3(4)'s requirements are operationally infeasible today for mobile ALPR systems, as they are designed to continuously capture data and cannot be toggled by location.

For agencies using Fleet 3, the key product implication is that ALPR use is something that must be affirmatively enabled and managed. If an agency determines that ALPR should not be operating in a given environment, the relevant way to stay within policy is to disable ALPR collection rather than assume that muted alerts or inactive screens stop collection. Agencies have several ways to do that in Axon products:

- Disable ALPR per Fleet 3 device in Axon Evidence where device-level control is sufficient.
- Work with Axon to disable ALPR-related feature flags where the goal is to stop broader ALPR sharing or Vehicle Intelligence functionality.

Once ALPR is fully disabled, users will no longer see the ALPR icon in Fleet Dashboard. If that icon is visible, the feature is active and plate reads are being captured.

This section also matters for agencies using Fusus. Turning off Fleet 3 ALPR does not disable third-party ALPR access through Fusus. If an agency needs to stop ALPR querying entirely, it must separately disable any plate-search integrations in Fusus, including the Flock Safety Plate Search integration under Admin > Integrations > API, and delete any associated credentials.

### Section 5(6): Technical controls preventing unauthorized sharing, secondary transfer, or access

In Axon products, agencies can operationalize this requirement by reviewing and controlling:

- user permissions
- role-based access
- sharing-related feature flags
- inbound and outbound integrations
- webhooks and partner API connections

ALPR data in Axon is not automatically shared outside the originating agency. Sharing is opt-in and must be explicitly enabled. That means agencies can stay within policy by keeping sharing disabled unless they have affirmatively decided to allow a specific workflow.

For third-party partner data such as Flock, Peregrine, or Vigilant, the same principle applies: if that data is ingested into the Axon environment, agencies should review whether those integrations are active and whether they should remain active. Where an agency wants to eliminate external ALPR data pathways, it should:

1. remove inbound ALPR integrations so those results are not available to users, and
2. review outbound integrations, webhooks, and partner APIs to confirm no data is flowing to external partners.

### Section 5(7): Preventing unauthorized access to ALPR data

Section 5(7) prohibits vendors from allowing access to ALPR data by unauthorized agencies, people, or entities. For agencies using Axon products, this requirement is implemented through the way access is granted inside the environment. The practical compliance step is to review users, admins, groups, and integrations that can touch ALPR data and reduce that access to only what is intended.

Agencies should use permissions to:

- remove ALPR-related feature access from users who do not need it
- review admin roles that can enable sharing or integrations
- disable plate-search integrations that are no longer appropriate
- confirm that data is not being exposed through partner connections or API pathways the agency no longer intends to use

### Section 5(8): No changes to sharing permissions without the agency's knowledge or explicit consent; default settings must prevent unauthorized sharing

This section has two practical implications for agencies:

1. sharing settings must remain under agency control, and
2. agencies should verify that their environment is configured to a restrictive default state unless sharing has been intentionally approved.

Axon's sharing architecture supports this by requiring affirmative enablement before sharing capability is active for an agency. Sharing features exist in the product, but it does not become active for a customer unless the relevant functionality is intentionally enabled for that agency and the sharing and receiving agency both agree.

- keep sharing-related feature flags disabled unless specifically needed
- restrict who has administrative authority to request or activate sharing-related functionality
- periodically review whether sharing permissions remain appropriate
- confirm after changes or updates that no new sharing path has been introduced into the agency's workflow

This is also where agencies should review any external data paths created by integrations.

### Section 7(2)(ii): Annual reporting obligations

Section 7 requires agencies to submit and publish an annual report covering a range of ALPR-related activity, including enforcement outcomes, recoveries, preservation and disclosure activity, data sharing, warrant-based access, policy changes, internal audit results, total system activity, and camera locations.

Axon products can serve as the source of much of the system-created data relevant to these reporting categories when agencies use the available workflows and records consistently.

### Matches resulting in stops, arrests, prosecutions, and recoveries

Agencies can capture and preserve the underlying ALPR activity associated with these reporting categories through Fleet 3 alerts, hit records, and related workflow activity. Where cleaner reporting outputs are needed, structured workflows in Fleet 3 and Fusus can be used to connect ALPR-generated events to downstream operational actions.

As Fusus workflows continue to expand, outcome tracking can be further supported through standardized alert handling and status-based actions, such as marking the result of an ALPR-related alert. This creates a more consistent system record showing how ALPR activity connected to a later event.

### Preservation requests and disclosure orders

The platform can generate and preserve supporting records that help agencies compile these counts later. Audit logs, exports, case-linked records, and retained access history provide system-generated evidence showing what data existed, how it was accessed, and what records were available for preservation or disclosure.

### Sharing with or access by another governmental entity

Reporting-relevant data for this category can be drawn from access logs, sharing-related activity, and audit records showing when ALPR data or related records were accessed or exported. Where access occurs through controlled sharing paths or interagency workflows, those actions can appear in audit data that agencies can later use to identify sharing activity and the entities involved.

### Access pursuant to judicial warrant

This category can be supported through audit and access records tied to the underlying search, export, or access event. If agencies use consistent case association, tagging, or categorization practices in the product, those records become much easier to isolate for reporting purposes.

### Policy changes affecting collection, retention, access, or sharing

Axon products do not create policy documents, but they do preserve the underlying configuration state and system behavior relevant to those policies. Changes to retention settings, sharing-related controls, user permissions, and enabled integrations can be reflected in the current system configuration and supporting audit or admin records. That gives agencies product-level evidence of how ALPR controls were configured during the reporting period.

### Results from the agency's internal audit

Audit trail data generated in the system can support an internal audit, including records of searches, access activity, exports, and other relevant actions. Those logs do not replace the agency's audit conclusions, but they do provide the system-created source data needed to conduct the review and document what occurred during the reporting period.

### Total annual reads, searches with results, and alerts

System generated activity records can be used to count:

- total ALPR reads
- searches performed
- search results and hit activity
- alerts generated

### Locations of cameras used as part of the ALPR system

This reporting category can be supported through device exports and associated device records that include location-related information for deployed cameras. Those records provide system-generated device data that can be used to compile the camera location portion of the annual report.

### Axon-created data relevant to Section 7

Taken together, Axon workflows and records can generate and preserve reporting-relevant data across the following categories in Section 7:

- ALPR reads
- hit and alert activity
- search activity
- access history
- export and sharing-related audit data
- case- or workflow-linked system activity
- configuration data relevant to retention, sharing, and access settings

### Section 8(1): Audit trail data documenting access to the system

Section 8 requires agencies to retain audit trail data showing how the system was accessed and used. That includes the identity of the user, the date and time of the access, data elements used to query the system, the purpose of access, case or call information, and the location of the camera involved.

In Axon products, agencies can support this through existing logging in Evidence.com and Fusus.

Agencies should use these systems to preserve and review:

- who ran a search
- what agency they belonged to
- when the search occurred
- what search values were used
- what contextual fields were entered in support of the search

Evidence.com already supports a dedicated Offense Category field for ALPR searches. Fusus is also being enhanced to better capture fields like offense category and case number in a more structured way.

### Section 8(1)(a): Records of access and searches

Evidence.com and Fusus generate audit records that capture core search and access activity, including the identity of the user, the agency associated with that user, the date and time of the activity, and the values used in the search. These records provide the foundation for the audit trail data contemplated by Section 8.

The statute also calls for the purpose of access, including offense type for criminal investigations, along with the associated call for service or case number. Evidence.com already supports a dedicated Offense Category field for ALPR searches.

Additional product enhancements in Fusus are intended to support more structured capture of fields such as offense category and case number, making the audit record more closely aligned to the format contemplated by the law.

Where those structured fields are used as part of the search workflow, the resulting audit data becomes more complete and more useful for later review.

### Section 8(1)(a)(vi): Location of the cameras accessed

Section 8 also calls for audit trail data that includes the location of the cameras that are part of the ALPR system accessed.

Camera location and device information is captured at the time of each read. However, our current audit log infrastructure does not easily allow for an audit report that consolidates this information. Axon is currently exploring options to implement this enhancement to the audit trail to satisfy this external reporting requirement in time for the December 2027 deadline to report out on this information and will have a committed schedule to share by May 15.

### Section 8(1)(b): Exports, downloads, and sharing

Axon evidence.com generate audit and export-related records that can support this requirement by showing when ALPR-related information leaves the platform or is otherwise made available beyond the initial search or access event, and this will be available on Fusus searches in the coming months. These records provide the system-created basis for reviewing export and sharing activity as part of annual audit and compliance workflows.

This category can also be informed by enabled integrations, outbound connections, and other configured data paths that affect how ALPR-related information moves through or out of the environment.

### Section 8(1)(c): Vendor-generated audit trail data

The statute requires agencies to obtain and retain any audit trail data generated by or made available through a third-party vendor providing ALPR system services.

Axon products support this by making audit-related records available for review and export. Audit outputs from Evidence.com and Fusus can be preserved as part of the agency's broader audit record, giving the agency access to vendor-generated system data in a retrievable form that can be retained over time.

### Section 8(2): Query data retained solely for auditing purposes

Section 8 states that data elements used to query the ALPR system and retained as audit trail data may be used only for auditing purposes and may not be searched, analyzed, compiled, or indexed for investigative purposes. It also requires partial redaction of unique identifiers in any public disclosure.

Axon products support this distinction by separating operational search activity from audit and export workflows. Query values captured in audit records can be retained as part of the compliance record, while audit outputs remain distinct from the operational search interfaces used for investigative work. Those same audit outputs can also be reviewed and prepared for disclosure through the agency's normal redaction process where public production is required. Additionally, audit functionality is restricted to ALPR Administrators within the agency, providing an added layer of permissions and ensuring this capability is only visible and accessible to a limited, authorized subset of users.

### Section 8(3): Annual internal audit

Section 8 requires an internal audit at least once each year reviewing access to and use of the ALPR system, along with compliance with retention, purging, and sharing requirements.

The records generated in Axon products provide the underlying source material for that review, including search history, access activity, export records, and system configuration relevant to retention and sharing. Because those records are created in the normal course of product use, they can serve as the system-generated basis for evaluating how the ALPR environment was used during the reporting period.

### Retention and purge settings across the bill

In Axon Evidence, plate reads and plate hits each have their own retention setting. They are configured independently. Setting one to zero does not affect the other. If the goal is to ensure neither persists in the cloud, both must be set to 0 days.

The configurable range is 0 to 1,825 days. Once the configured retention period expires, the record is removed from search results immediately and permanently deleted through the cleanup process. It cannot be restored.
For agencies seeking the most restrictive posture, the practical setup is:

- set reads retention to 0
- set hits retention to 0
- verify ALPR is disabled where needed at the feature or device level
- remove integrations that could still expose third-party ALPR data

## What happens on the vehicle

ALPR reads and hits captured by Fleet 3 are stored locally on the Hub and automatically uploaded to the cloud approximately every 15 seconds. The Hub will remove a local copy of a record once it has been successfully uploaded and is more than 24 hours old. If the Hub approaches its storage limit (3,000 uploaded records), older uploaded records may be cleared sooner to free up space.

That means the most restrictive end-to-end set up for ALPR data is achieved by:

- disabling ALPR where required,
- setting both reads and hits retention to 0, and
- removing any remaining integrations that still provide ALPR access.

## Recommended agency review based on SB 6002

To align an Axon environment with SB 6002, agencies should review the following product areas:

- Fleet 3 device-level ALPR enablement
- ALPR-related feature flags
- reads retention and hits retention
- user roles and ALPR search permissions
- sharing settings
- Fusus integrations, including Flock Plate Search
- outbound webhooks and partner APIs
- audit export and retention workflow
- structured use of offense category, case number, and related search context
- annual reporting workflow built from system records

## Axon's ongoing product work

Axon is continuing to improve the product workflows that support auditability, reporting, and review under requirements like those in SB 6002. This includes work related to:

- expanded device visibility across ALPR device types
- improved categorization for alert and search workflows
- more unified audit review across systems
- more usable exports for annual review and reporting
- additional transparency-oriented reporting support

As these enhancements are released, they will further improve how agencies can operationalize SB 6002 requirements directly within Axon software.