Table of Contents

Axon Products & EU Data Protection Reform ........................................................................................................3
GDPR & LED Primer ...............................................................................................................................................3
   The GDPR ......................................................................................................................................................3
   The LED .......................................................................................................................................................3
   What does GDPR and the LED mean for Axon Products? .................................................................4
Axon Products – Data Protection Features ...........................................................................................................4
   Transparency & Right to be informed ...........................................................................................................4
   Recording Alert ........................................................................................................................................4
   Limited Access and Footage Security .......................................................................................................5
   Data Minimization & Storage Limitation ...................................................................................................7
   Capture only the moments that matter .......................................................................................................7
   Retain data no longer than needed ...........................................................................................................8
   Video Watermark .....................................................................................................................................8
   Forensic Fingerprinting and Integrity .......................................................................................................9
   Citizen Identity Protection .........................................................................................................................9
   Data Processing Records and Accountability ........................................................................................10
   Deletion process .......................................................................................................................................11
Certifications .....................................................................................................................................................11
Axon Products & EU Data Protection Reform

In 2018, EU data protection reform came into force. Within the legislative package was the General Data Protection Regulation (GDPR), which received abundant news coverage and industry awareness as it includes requirements for the processing of EU-citizen personal data.

However, the data protection reform also included a directive on protecting EU-citizen personal data processed for the purpose of law enforcement and criminal justice (the Law Enforcement Directive, or LED). The LED, which applies only to processing of personal data law enforcement and criminal justice data, did not receive the same coverage or industry awareness that accompanied the GDPR. Yet for Axon’s customers, the LED is the most applicable data protection reform for the processing of personal data for criminal law enforcement activities.

GDPR & LED Primer

The GDPR

This regulation sets out the rights of the individual and establishes the obligations of those processing and those responsible for the processing of the data. It also establishes the methods for ensuring compliance as well as the scope of sanctions for those in breach of the rules.

GDPR came into force on 25th May 2018, enabling consumers to understand and control processing of their personal data. Simply speaking, it gives every EU citizen the right to know what, why, where and when their data is being used as well as a new right ‘to be erased or forgotten’ (subject to exceptions), with non-law enforcement entities. The official GDPR text is located: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The LED

The Law Enforcement Directive aims to protect the right of individuals and the protection of their personal data while guaranteeing a high level of public security. It applies to both cross-border and national processing of data by member states’ competent authorities for the purpose of criminal law enforcement. Typically, any processing of data that qualifies under LED is not subject directly to GDPR provisions. That said, many of the same protections granted to citizens with the GDPR are similar under the LED.

However, a key difference between the GDPR and LED is how the reforms are integrated into member state law. The GDPR, being regulation, applies to all member states as written. On the other hand, as a directive, the LED must be transposed by member states into national law, which law will likely differ across the member states.
An example of GDPR and LED being implemented into national law is evident in the UK’s Data Protection Act of 2018

- General EU Data Protection Reform & GDPR inclusion and supplements: 

- Specific LED Implementation within the Data Protection Act of 2018:

### What does GDPR and the LED mean for Axon Products?

Axon believes the adoption and focus on data protection and privacy regulation strengthens the need for secure and robust digital evidence data collection, management, and sharing functionality within law enforcement.

Axon is confident that Axon Products enable customers to implement governance over the handling and sharing of digital evidence to meet their requirements under GDPR and the LED as transposed into Member State national law. Below, in Axon Products – Data Protection Features, a selection of specific product design and functional features are outlined.

Beyond current product design and functionality, Axon is committed to continuing to develop and enhance Axon’s products to ensure customers can meet data protection and privacy expectations from their communities and regulatory environment when using Axon products.

However, regardless of available design and functionality within Axon products, Axon recommends that customers work with their legal counsel to determine if national, state, or local laws affect their current processes and policies.

Additionally, Axon employs a data protection and privacy group that is available for customer discussions and assistance. Please contact your local Axon representative or privacy@axon.com.

---

### Axon Products – Data Protection Features

#### Transparency & Right to be informed

**Recording Alert**

Axon cameras can be marked with warning labels, indicating that the device records audio and video so that citizens are aware that they can be recorded in case of incident (for example: very useful in situations as soccer stadiums or demonstrations);
The camera can be configured so that when in recording mode a red light will bling in the main body of the camera making it quite visible that the camera is recording:

**Figure 1 Axon Body 2 camera**

Axon cameras, unlike sports cameras, do not have a front screen. Therefore, what is recorded can be made not accessible for viewing (neither by the agents carrying the cameras, nor by the citizens passing by). Axon View functionality can be disabled organizationally.

**Limited Access and Footage Security**

Figure 2 Axon Body 2 camera recording (front ring red)
The absence of a front screen, granular role-based permissions in Axon Evidence and control over Axon View pairing, ensures that the images captured by the camera can only be viewed in the system and by authorized people. Thus, it is possible to configure the system such that the images recorded by these cameras cannot be seen by the agent who recorded them, nor by the citizens.

The video recording in the camera is kept in the internal memory of the camera to which the user does not have direct access to. The camera has a proprietary file storage format and does not natively mount as a drive within operating systems.

The videos are offloaded through Axon Docks that encrypts the video for data transmission. When the agent returns to the station, he or she places the camera in a Dock that is directly connected to the network. This Dock not only charges the camera, but also uploads the videos from the camera to Evidence.com, with the videos being deleted from the camera once the system checks the correct transmission of the images. As the Dock is directly connected to the network, the data does not have to go through a workstation or laptop.

The videos are sent to their central storage Axon Cloud Services and are kept encrypted in the system. Access to the videos can only be done through the Axon Cloud Services systems.

Axon Cloud Services has an access control mechanism. Customers define who can watch the videos, who can classify them, etc. If so desired, an agent can only be the carrier of the body camera and may never see the images that his camera recorded.
Capture only the moments that matter

Axon cameras are designed to record incidents and not capture full shifts of activity. The cameras when turned on stay active (in standby), but not recording. You can activate the pre-buffer mode that causes the camera to save video in volatile memory (ie, RAM), but retaining only a customer-defined pre-buffer timeframe (e.g. the previous 30 seconds). That is, the camera rewrites the last
30 seconds in dynamic memory. If no recording occurs during the work shift, the camera will not have any video.

In case of an incident (theft, aggression, etc.) the agent presses the record button and in that instant the pre-buffer from the volatile memory are retained to provide assurance that the full incident, pre-context and its context are recorded.

This approach helps minimize the amount of data being captured while providing functionality to retain the whole context of the incident.

Examples of how the pre-buffer mechanism works:

- An agent patrols a street and sees a theft of a lady purse. In that moment he presses the button to start recording. However, when starting the recording, the theft already occurred. That is why the camera adds to the video the pre-buffer before the beginning of the recording, which will allow to have the registry of the moments previous to the theft and of the theft itself, in order to record the whole episode and the context related to the incident.

- An agent watches a car hit and run. By pressing the record button and the car has already run away. However, since the camera has the pre-buffer retained, this video is added to the video record, being able to give the information of the whole incident, as well as the identification of the vehicle and possibly the driver.

This mechanism of pre-recording allows the camera to be active without being permanently recording which could pose a threat to the privacy of citizens.

<table>
<thead>
<tr>
<th>Retain data no longer than needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories within Axon Evidence provides the ability to create policies, maintain them, and assign them to evidence. Categories include policy settings for evidence retention and restricted access for especially sensitive evidence. This capability enables customers to retain data in directly alignment with customer-defined data retention policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Video Watermark</th>
</tr>
</thead>
<tbody>
<tr>
<td>The images collected by Axon cameras have a watermark with the Axon logo. This water provides identification of the camera, the date and time of each frame. This watermark as well as specific metadata stored within Axon camera multimedia containers mitigate manipulation of the frames.</td>
</tr>
</tbody>
</table>
Forensic Fingerprinting and Integrity

Forensic fingerprint of each evidence file using industry standard SHA hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission. The SHA hash is retained with the evidence audit trail throughout the lifecycle of the evidence file in Axon Cloud Services.

Citizen Identity Protection

Axon Cloud Services allows masks to be placed on the face of people, children, etc. In the previous example, where only the driver of the vehicle who made the attack is to be identified, masks may be placed on the faces of other drivers or anonymous citizens appearing in the video before sharing it with other acting forces.
The system always keeps the original video, which can be requested by a court judge for complementarity of facts.

**Data Processing Records and Accountability**

All the actions carried out in the system with the video, from its upload, any viewing, cataloguing, redaction (facial masks) to protect the privacy of citizens, sharing, and deletion, remain registered in the system and can be audited at any time. The logs include the action, the date of the action, and its author. The system has two audits:

- Video Audit: all actions taken in this video, who recorded it, who uploaded it to the system, who and when viewed, catalogued, etc.;
• User Audit: for each user it is possible to have an audit of all the actions carried out in the system.

![Figure 10 Video Audit](image)

**Deletion process**

All videos marked for deletion will go through a quarantine period and are not actually deleted until the quarantine period of 7 days elapses. Even when a video is deleted, the file with the audit of everything that happened with the video remains in the system.

**Certifications**

Axon Cloud Services are certified or comply according to the following standards:

- ISO/IEC 27001:2013 Certified
- ISO/IEC 27018:2014 Certified
- FBI CJIS Security Policy Complaint
- SOC 2+ Reporting
- Cloud Security Alliance STAR Level 2

Axon’s compliance demonstrates our commitment to providing a trustworthy platform and offers customers a way to understand the controls that have been put in place to secure Axon Cloud
Services and their data. Learn more about Axon’s Security Program and Compliances at: https://global.axon.com/trust