Axxon One VMS

GDPR Compliance Overview

2024

Disclaimer

This document is intended solely as a general guide to understanding how Axxon One VMS aligns with GDPR requirements and incorporates privacy-enhancing features. It is provided 'as is' without any express or implied warranties, including but not limited to, warranties of merchantability, fitness for a particular purpose, or non-infringement. It is not intended to serve as legal advice or a comprehensive analysis of GDPR compliance obligations. Organizations using Axxon One VMS are responsible for ensuring that their use of the system complies with all applicable data protection laws and regulations.

AxxonSoft disclaims all liability for any damages arising out of the use or inability to use the information provided in this document. Nothing in this document should be construed as constituting a warranty, guarantee, or legal advice. Users of Axxon One VMS are solely responsible for ensuring that their use of third-party components complies with all applicable laws and regulations, including GDPR and other relevant data protection laws. AxxonSoft reserves the right to make adjustments and updates to the content without prior notification. All names of individuals and organizations used in examples are fictitious, and any resemblance to actual persons, living or dead, or to real organizations, is purely coincidental and unintended. Users are responsible for regularly reviewing this document and ensuring that their use of Axxon One VMS remains in compliance with the most current version.

AxxonSoft does not assume any liability for legal outcomes or decisions based on the information provided in this document. It is recommended that organizations consult with legal counsel or a data protection officer to obtain specific legal advice tailored to their particular circumstances and to ensure full compliance with GDPR and other relevant privacy laws.

Please be aware that this product may utilize third-party software components, each of which may be subject to specific terms and conditions. Users must independently verify that their use of third-party software components within Axxon One VMS is compliant with all applicable laws and licensing agreements.

Content

1. Introduction and General Description of the Product

This document outlines how Axxon One VMS supports compliance with the General Data Protection Regulation (GDPR), including key features, functionalities, and best practices.

Axxon One VMS is a highly adaptable and scalable video management software solution tailored to meet the diverse needs of modern surveillance systems. Designed for both small-scale installations and large, multi-site deployments, Axxon One VMS combines advanced video analytics with Artificial Intelligence (AI) to deliver unparalleled security and operational efficiency. Its intelligent video management capabilities are supported by customizable features that allow users to tailor the system to specific operational requirements, ensuring optimal performance in any surveillance scenario.

The software is built with a strong emphasis on data protection and privacy, making it an ideal choice for organizations that must comply with stringent regulations such as the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Key privacy-enhancing features include Privacy Masking, which automatically blurs individuals and objects in video footage to protect personal data. Additionally, Axxon One VMS incorporates robust encryption protocols for both data in transit and at rest, along with comprehensive Role-Based Access Control (RBAC) to ensure that only authorized personnel have access to sensitive information.

In the context of GDPR compliance, Axxon One VMS offers a suite of tools designed to help Data Controllers and Data Processors as defined under GDPR, specifically under Articles 4(7) and 4(8) fulfill their legal obligations. These include configurable data retention policies, detailed audit logs, and mechanisms for managing data subject access rights, all of which support the lawful and secure processing of personal data. While Axxon One VMS provides the technological framework to facilitate compliance, the ultimate responsibility for ensuring adherence to GDPR rests with the entities that deploy and manage the system. AxxonSoft, as the software provider, is neither a Data Processor nor a Data Controller under GDPR, and thus the legal obligations for compliance remain with the system's operators. These entities are obligated to comply with GDPR provisions, including but not limited to:

1. Article 5 - Principles relating to processing of personal data, ensuring lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
2. Article 6 - Lawfulness of processing, where they must ensure that personal data is processed lawfully, based on valid legal grounds.
3. Article 7 - Conditions for consent, requiring valid consent from data subjects when necessary.
4. Article 25 - Data protection by design and by default, which mandates the implementation of appropriate technical and organizational measures.
5. Article 30 - Records of processing activities, requiring Data Controllers and Data Processors to maintain detailed records of all processing activities.

6. Article 32 - Security of processing, mandating that entities implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
7. Article 33 - Notification of a personal data breach to the supervisory authority, where Data Controllers must notify the relevant supervisory authority within 72 hours of becoming aware of a breach.
8. Article 35 - Data protection impact assessment (DPIA), where Data Controllers must assess the impact of processing operations on the protection of personal data when introducing new technologies or systems.
9. Article 44 - General principle for transfers of personal data to third countries, which ensures that any international data transfers comply with GDPR requirements

In the context of GDPR and CCTV systems, the key stakeholders are:

1. Data Controller: The entity or individual that determines the purposes and means of processing personal data captured by the CCTV system. This is typically the organization that owns or operates the surveillance system, such as a business or public authority.
2. Data Processor: A third party that processes personal data on behalf of the Data Controller. In CCTV scenarios, this could be a company contracted to monitor, store, or analyze the footage, but not usually a vendor, which only provides the software.
3. Data Subject: Individuals captured on CCTV footage whose personal data is being processed. They have rights under GDPR, such as access to their data and the right to request its deletion.

Each of these stakeholders has specific responsibilities and rights under GDPR to ensure the lawful processing and protection of personal data. AxxonSoft explicitly disclaims any responsibility as a Data Controller or Data Processor as defined under GDPR.

In the context of CCTV systems, a Data Subject is any individual who is captured on camera, and whose personal data is being processed through video recording. Under the General Data Protection Regulation (GDPR), Data Subjects have several rights aimed at protecting their personal information and privacy. These rights include the right to access their data (Article 15), the right to rectification if their data is incorrect (Article 16), the right to erasure (also known as the right to be forgotten) (Article 17), and the right to restrict or object to certain processing activities (Articles 18 and 21). Organizations operating CCTV systems must ensure that these rights can be exercised by providing clear information about the data processing activities, including how individuals can request access to their footage or lodge a complaint.

Furthermore, organizations must implement appropriate measures to safeguard the privacy of Data Subjects, such as using Privacy Masking to blur individuals in the video footage where necessary. The principle of data minimization (Article 5(1)(c)) also applies, meaning that CCTV systems should only capture and store footage that is necessary for the intended purpose, and that footage should not be retained longer than required (Article 5(1)(e)). Data Subjects must be informed of the presence of CCTV cameras,

typically through visible signage, which should include details about the purpose of the surveillance, the identity of the Data Controller (Article 13), and how to exercise their rights under GDPR.

2. Axxon One to reduce the impact on the right of the Data Subject

Axxon One VMS is designed with several features and functionalities that actively reduce the impact on the interests or fundamental rights of the Data Subject, in line with GDPR requirements:

1. Privacy Masking: Axxon One includes advanced Privacy Masking capabilities, which automatically blur individuals and objects in the video footage. This feature helps to ensure that personal data, such as identifiable facial features or license plates, is protected from unauthorized viewing. By obscuring sensitive information, Axxon One minimizes the risk of infringing on the privacy rights of individuals captured on camera.
2. Role-Based Access Control (RBAC): The system employs a robust RBAC mechanism that restricts access to video footage based on user roles. Only authorized personnel can view unmasked video, ensuring that personal data is accessible only to those with a legitimate need. This controlled access prevents unnecessary exposure of personal data and aligns with the GDPR principles of data minimization and purpose limitation.
3. Configurable Data Retention Policies: Axxon One allows organizations to set data retention policies that automatically delete video footage after a specified period. This feature ensures that personal data is not kept longer than necessary, reducing the risk of misuse or unauthorized access, and complying with GDPR's requirement for data minimization and storage limitation.
4. Encryption and Secure Data Handling: The system implements strong encryption protocols for both data in transit and at rest, ensuring that video footage is securely protected from unauthorized access. By safeguarding personal data through encryption, Axxon One reduces the potential impact on the data subject's privacy and security.

While Axxon One VMS provides the technological framework to facilitate compliance, the ultimate responsibility for ensuring adherence to GDPR rests with the entities that deploy and manage the system. Through these measures, Axxon One VMS significantly reduces the potential impact on the fundamental rights and freedoms of Data Subjects, ensuring that their privacy is respected and protected in compliance with GDPR.

3. Data Protection Impact Assessment (DPIA)

Axxon One VMS includes advanced functionalities such as facial recognition and AI-based analytics that may require a Data Protection Impact Assessment (DPIA) under GDPR Article 35. It is the responsibility of the Data Controller to conduct a DPIA when using Axxon One VMS in a way that could pose high risks to data subjects' rights and freedoms.

4. Confidential and Tamper-Proof Video Data Export

Axxon One VMS ensures that exported video data, including privacy masks, remains confidential and tamper-proof. Exported video files merge video and privacy mask layers, making it impossible to remove privacy masks post-export. Only authorized roles can export unmasked video, and additional privacy masks can be configured if required.

When exporting a part of the archive with masked areas of the frame on the server, the video layer and the layer with privacy masks are merged into a single video sequence and written to the final file. Accordingly, it is impossible to get rid of privacy masks in the exported video file.

It is important to note that users belonging to roles without access to viewing masked video during export will automatically receive all privacy masks generated by analytics, both in the export editor and in the final video file. At the same time, for users belonging to a role with access to viewing masked video, privacy masks generated by analytics will not be displayed in the export editor and will not go to the final video file without manually adding them.

If an additional privacy zone is required or a mask is manually added, the export editor provides a function for adding and configuring additional privacy masks. The export editor has the ability to customize the mask shape and its behavior (dynamic or static).

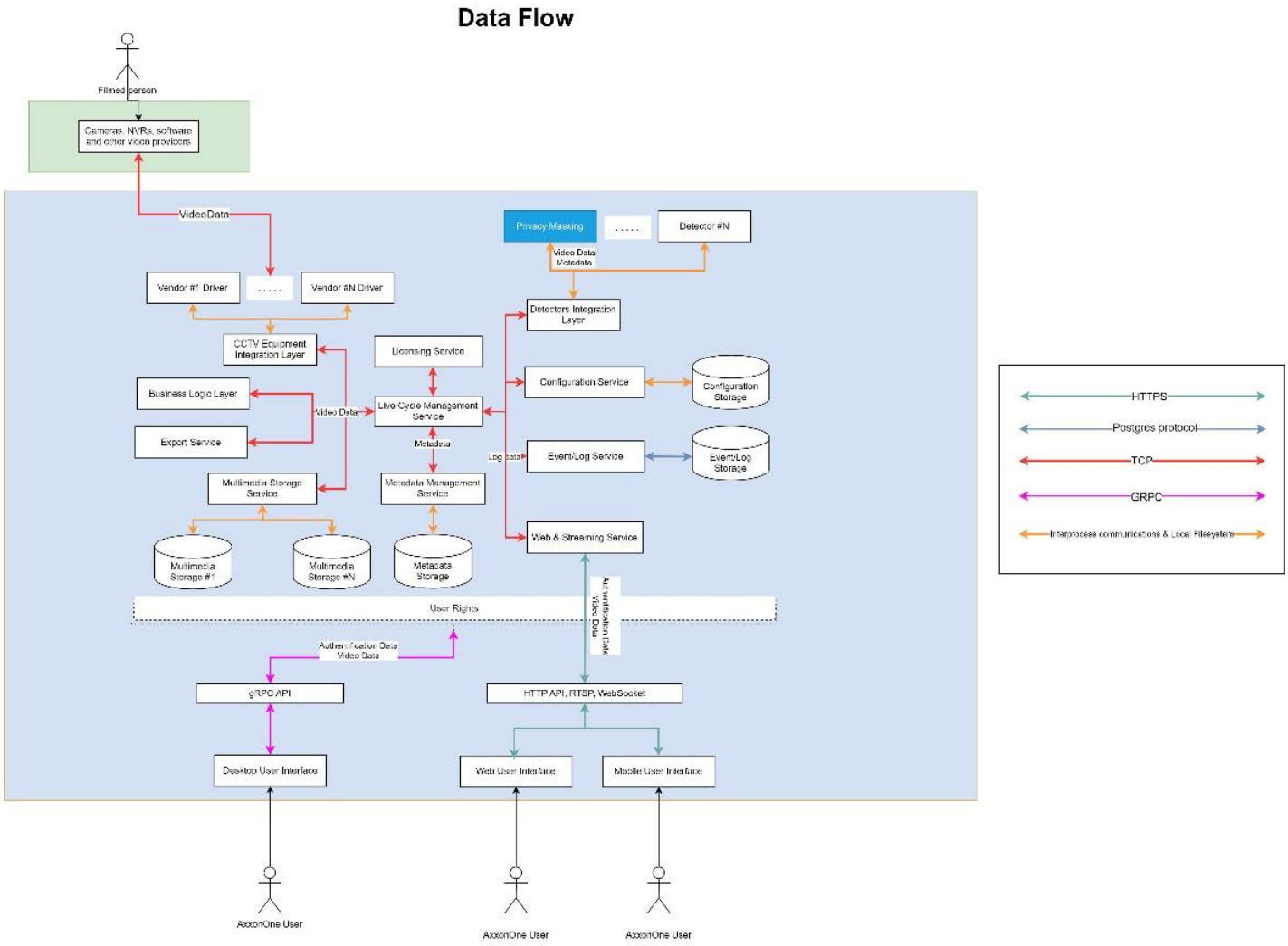
5. Confidential and Tamper-Proof Transport and Storage of Video Data

- Privacy Masking in Metadata: Privacy masks are stored as metadata in a separate video layer, ensuring that only users with appropriate role-based permissions can view unmasked video.

- Technical Impossibility of External Access: Axxon One VMS does not support broadcasting unmasked video to third-party systems, preventing unauthorized access from outside the system.

6. Data Flow in Processing

Axxon One VMS processes video data in a secure environment, with privacy masks applied where necessary to protect personal data. AxxonSoft disclaims any liability arising from misconfiguration or misuse of these features. The Data Controller and Data Processor are responsible for ensuring that data processing activities comply with GDPR requirements.



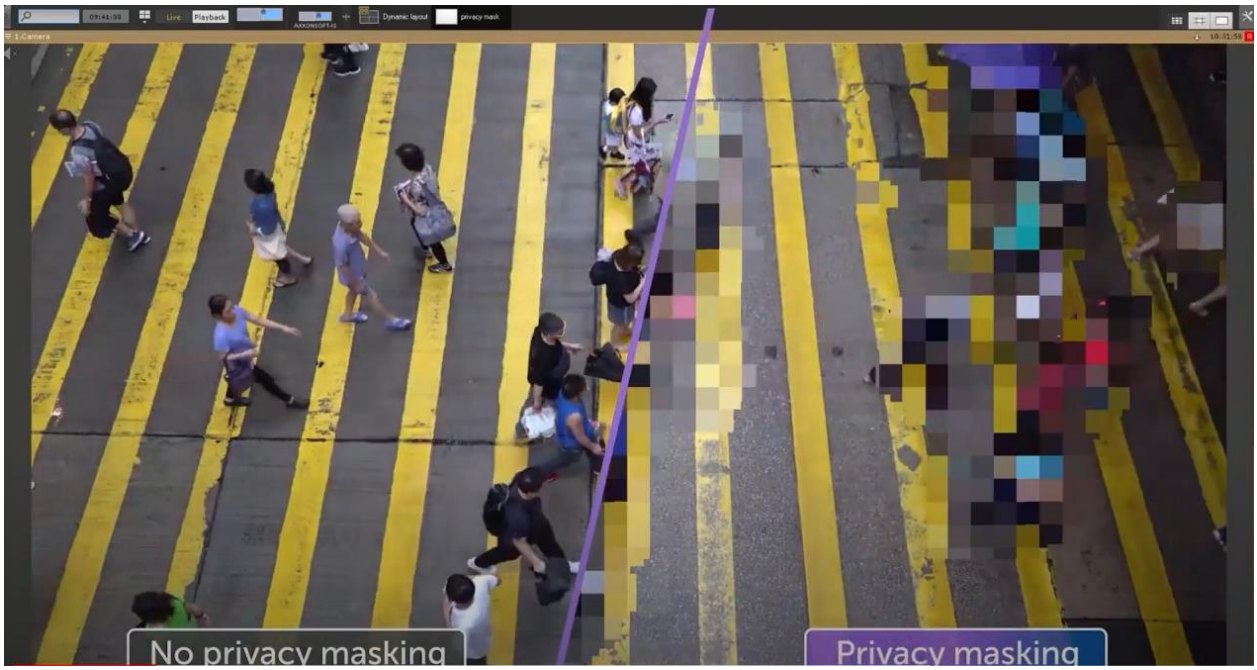
7. Privacy-Enhancing Functionalities

Axxon One VMS includes several privacy-enhancing features:

- Dynamic and Static Privacy Masks: Automatically blur parts of the video frame containing moving objects or people, and configurable static masks for specific areas.

- Facial Recognition: Can be configured to mask detected faces within the video frame, ensuring that personal data is protected from unauthorized access.

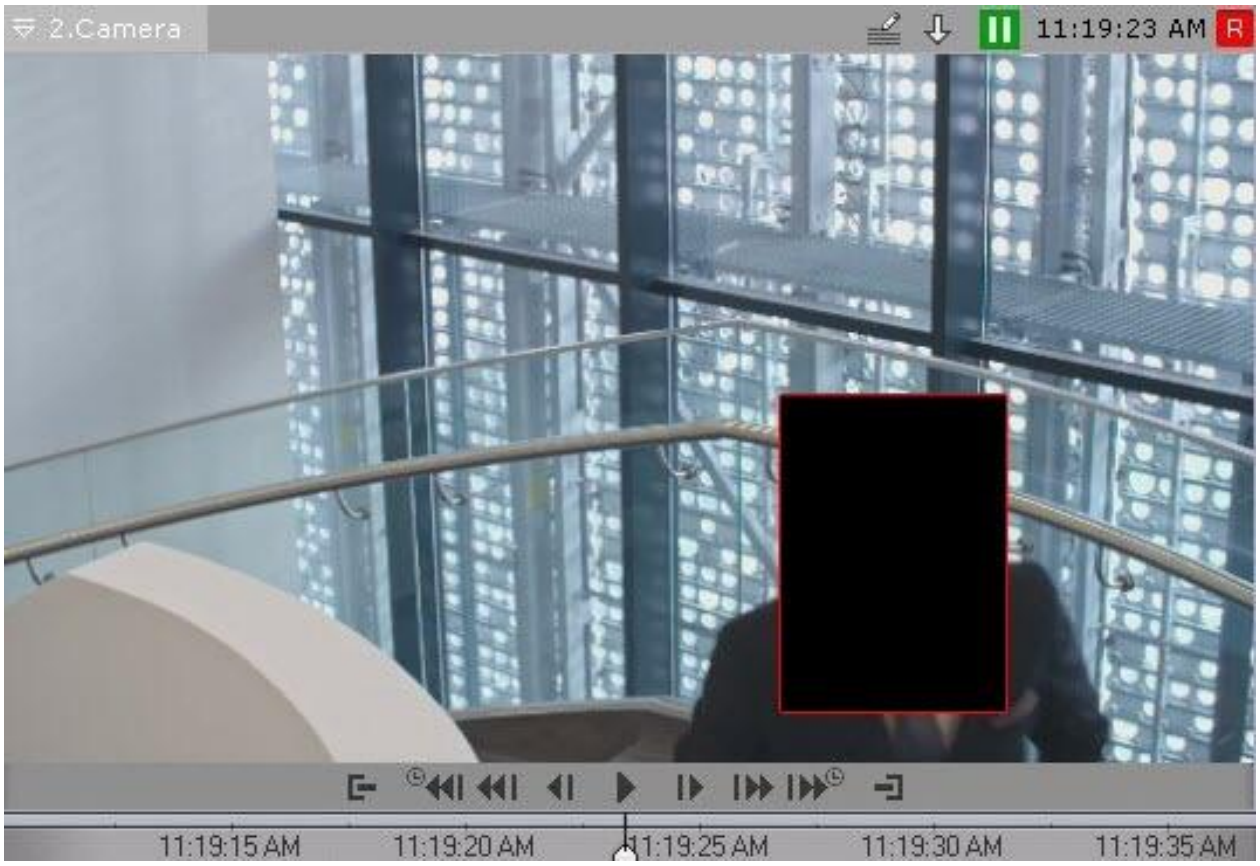
The Privacy Masks feature allows you to blur parts of a frame with moving objects and people in a video frame based on background changing technologies and a human neurotracker.



As an additional measure to protect personal data, sometimes it is necessary to mark a certain area of the video frame as a permanent privacy mask. Such an area can be easily configured using the Privacy Mask settings in AxxonOne.

In some security systems built with AxonOne, face recognition is an important and necessary function (for example, a passage group in a public place). To maintain confidentiality and protect personal data, the Privacy Masks function allows you to configure video masking based on detected faces within the video frame, hiding them

from ordinary users who do not belong to a special role.



8. Axxon One VMS Features Supporting GDPR Compliance

8.1 Data Encryption

- In Transit: Data is encrypted using HTTPS and TLS protocols to secure transmission between devices and servers.

- At Rest: Data stored within the VMS is encrypted with robust algorithms to prevent unauthorized access.

8.2 Access Control

- User Authentication: Multi-factor authentication (MFA) ensures only authorized users can access the system.

- Role-Based Access Control (RBAC): User permissions are assigned based on roles, ensuring that data is only accessible to those with the appropriate clearance.

8.3 Data Minimization and Retention

- Configurable Retention Policies: Data retention periods can be set to automatically delete personal data after a specified period, aligning with GDPR's data minimization principles (Article 5(1)(c)).

- Selective Recording: Users can configure the system to record only necessary data, reducing the volume of personal data processed.

8.4 Data Subject Access Rights

- Data Retrieval: Tools to easily locate and retrieve data related to specific individuals upon request, supporting compliance with Article 15 (Right of access by the data subject).

- Data Export: Allows personal data to be exported in a commonly used, machine-readable format, as required by GDPR.

- Data Deletion: Options to permanently delete data upon request, ensuring compliance with the right to erasure (Article 17).

8.5 Audit Logs

- Comprehensive Logging: All user activities are logged, providing a detailed audit trail for transparency and accountability.

- Tamper-Proof Logs: Logs are protected against tampering, ensuring their integrity and reliability.

8.6 Incident Management

- Real-Time Alerts: Immediate notifications of suspicious activities facilitate a quick response to potential security incidents.

- Incident Reporting: Integrated tools for documenting and reporting security incidents in compliance with GDPR requirements.

8.7 Axxon One: Privacy by Design

Axxon One VMS is engineered with a "Privacy by Design" approach, ensuring that privacy considerations are integrated into the core of its architecture and functionality. AxxonSoft shall not be liable for any compliance issues arising from improper configuration. This commitment to Privacy by Design means that Axxon One not only meets regulatory requirements like GDPR but also prioritizes the protection of personal data from the outset.

1. Built-In Privacy Features: Axxon One incorporates advanced privacy features such as Privacy Masking, which automatically blurs identifiable individuals and objects in video footage. This feature ensures that personal data is protected at the point of capture, reducing the risk of unauthorized access or exposure.

2. Data Minimization: The system is designed to process only the minimum amount of personal data necessary for its intended purpose. Configurable

settings allow users to limit recording to specific areas, times, or events, thereby minimizing unnecessary data collection and aligning with the GDPR principle of data minimization.

3. Secure Data Handling: Axxon One employs strong encryption protocols for both data in transit and at rest, ensuring that personal data is securely protected throughout its lifecycle. Additionally, Role-Based Access Control (RBAC) restricts access to sensitive data, ensuring that only authorized users can view unmasked footage.

4. User-Centric Controls: The software provides tools for Data Controllers and Data Processors to manage data retention, access rights, and audit logs, enabling compliance with GDPR while empowering organizations to respect the privacy of individuals. Features like configurable data retention policies ensure that personal data is not stored longer than necessary, while comprehensive logging provides transparency and accountability.

By embedding these privacy-enhancing technologies and principles into its design, Axxon One VMS not only facilitates compliance with data protection laws but also actively protects the fundamental rights of individuals, ensuring that privacy is a fundamental aspect of its operation from the ground up.

8.8 Encryption of Object Storage Volumes

- Object Storage Encryption: This functionality ensures that object storage volumes are encrypted, making it impossible to retrieve video and personal data even with direct access to the server's archive disks.

8.9 User Restrictions for GDPR Compliance (In process)

- GDPR-Specific Role Configuration: GDPR restrictions can be configured in role settings to limit access to personal data, such as:

- Face Recognition
- License Plate Recognition
- Similarity Search
- Vehicle Make/Model Recognition

9. Network Features Supporting GDPR Compliance

Axxon One VMS includes several network features that enhance security and compliance with GDPR requirements:

9.1 Secure Communication

- VPN Support: The system supports Virtual Private Networks (VPNs) to establish secure, encrypted connections between remote sites and the central server.

- TLS/SSL Encryption: Ensures that all data transmitted over the network is encrypted using TLS/SSL protocols to prevent interception and unauthorized access.

9.2 Network Segmentation

- VLAN Support: Virtual Local Area Network (VLAN) support allows administrators to segment the network, isolating sensitive data and reducing the risk of data breaches.

- Firewall Integration: Compatible with firewall solutions to monitor and control network traffic based on predetermined security rules.

9.3 Intrusion Detection and Prevention

- IDS/IPS Compatibility: Integrates with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect and prevent network-based attacks.

- Anomaly Detection: Built-in algorithms identify unusual network activity, indicating potential threats.

9.4 Network Monitoring

- Real-Time Monitoring: Provides tools for continuous network traffic monitoring to promptly detect and respond to incidents.

- Log Management: Centralized logging of network activity facilitates auditing and forensic analysis.

9.5 Remote Access Control

- Secure Remote Access: Administrators can securely access the VMS remotely via encrypted connections.

- Access Restrictions: Configurable settings restrict remote access based on IP addresses, user roles, and other criteria to minimize unauthorized access risks.

10. Mobile Agents Supporting GDPR Compliance

Axxon One VMS includes features in its mobile agents that enhance security and compliance with GDPR requirements:

10.1 Secure Mobile Access

- Encrypted Communication: All data transmitted between mobile agents and the VMS is encrypted, protecting against unauthorized access.

- Secure Authentication: Multi-factor authentication (MFA) is available for mobile access, ensuring that only authorized users can connect.

10.2 Data Minimization

- Selective Data Access: Mobile agents can be configured to access only necessary data, reducing personal data exposure.

- Local Data Storage Controls: Options to control or disable local storage of data on mobile devices, reducing risk in case of device loss or theft.

10.3 User Management

- Role-Based Access Control (RBAC): Mobile users are assigned roles that determine their access permissions, ensuring compliance with the principle of least privilege.

- Session Management: Tools for monitoring and managing active sessions, including remote termination of suspicious sessions.

10.4 Incident Reporting and Alerts

- Mobile Alerts: Immediate notifications of security incidents are sent to mobile agents for prompt response.

- Incident Documentation: Mobile agents include tools for documenting and reporting incidents from the field.

10.5 Remote Wipe

- Data Wipe Capability: Administrators can remotely wipe data from lost or stolen mobile devices to prevent unauthorized access.

10.6 Regular Updates and Patching

- Automated Updates: Regular updates and security patches are pushed to mobile agents to address vulnerabilities.

11.AxxonData of Axxon One Supporting GDPR Compliance

AxxonData is a free service for monitoring and managing on-premises Axxon One video surveillance systems that operates within closed local network environments without Internet access. This setup is referred to as a locally managed system. AxxonData provides convenient and secure remote video monitoring, custom report generation based on video analytics data, and centralized management of watchlists

for real-time facial and license plate recognition. Session with the AxxonData portal is HTTPS/TLS encrypted.

11.1 User Accounts Storage

- Account Security: User accounts are secured by encrypted passwords and confirmation via verification links. AxxonData stores only the necessary information (email address and encrypted password).

11.2 Face Lists and License Plate (LP) Lists

Face Lists

- Data Protection: AxxonData portal stores face lists information that are generated by user. It's not mandatory to store face lists on the portal.

Information that is stored:

- Name of a face list
- Image of a face
- Image name that is equals to the image file name
- Face creation date

Additional fields that user can update, and portal will same information:

- Surname
- Gender
- Age
- Title
- Department
- Comment
- Additional comment

By default, only list creator has access to the list. List creator can share the list with another user via email. It is technically impossible to access the list of persons and personal data from outside the system or under any other users with whom the list has not been shared.

LP lists

AxxonData portal stores LP lists information that are generated by user. It's not mandatory to store LP lists on the portal.

Information that is stored:

- Name of a LP list
- Palte number

Additional fields that user can update, and portal will sabe information:

- Comment

By default, only list creator has access to the list. List creator can share the list with another user via email. It is technically impossible to access the list of LP and personal data from outside the system or under any other users with whom the list has not been shared.

11.3 Reports and Dashboards

- Metadata Storage: Metadata generated by Axxon One analytics tools is stored for 90 days, allowing users to build reports and dashboards securely.