MAKE THE
WORLD SEE

Date: 6. Marts 2018

Frequently Asked Questions (FAQ)

GDPR READY

Prepared by:

Christian Brünniche Lund, Information Security & Compliance Manager, Global IT & Operations
Bjørn Bergqvist, Senior Product Marketing Manager, Product Marketing Management
Carsten Bøgelund, Security Architect, Research & Development

milestone

Table of Content

Introduction

This purpose of this document is to provide initial answers to questions regarding XProtect and GDPR compliance. It contains a variety of questions and answers discussing the scope of GDPR and compliance responsibilities in terms of the data stored and used, the data owner and processor, the geographical limitations, the product design and organizational implementation. Answers are given in context of Milestone's XProtect and not comprehensive.

Who is responsible for complying an XProtect VMS system with GDPR?

The direct responsibility for complying with the GDPR regulations is first and foremost the VMS owner's i.e. the data controller (end-user in most cases). In cases where there is a data processor involved e.g. a security company, the data controller and the data processor must have a Data Processor Agreement (DPA) in place, stating what data is processed, how is it protected, what is the retention period etc.

Is every video surveillance installation required to comply with GDPR?

GDPR protects the privacy of any resident of the geographical area of the European Union. GDPR covers all kinds of video surveillance taken within the EU and protects citizens of all countries who reside within the EU (GDPR article 3). This is defined based on the camera's physical location, regardless of whether the processing takes place in the EU or not. For example, if an EU-located camera or VMS installation is controlled or accessible by a non-EU-located VMS installation, making video data of an EU resident accessible for processing, the entire installation is subjected to comply with GDPR.

What types of personal data descriptions stored by XProtect, fall within the scope of GDPR?

GDPR operates on two levels of personal data: primary and secondary. Primary Personal Data is any type of information that directly or indirectly can be used to identity a natural person (data subject). This can be video surveillance streams, a single image or still motion combined with location information from cameras and/or layered maps, an access control integration identifying a personal access card and combining it with a specific location, or data from License Place Recognition (LPR) with or without any location data.

Notice that Primary Personal Data is defined as sensitive if the video surveillance is in close proximity to children (e.g. kinder garden), hospitals (related to health information), jails (criminal convictions), political activity (union membership), religious activity, or images that reveal sexual orientation (e.g. gay bars). Due to its sensitivity and potential misuse by the wrong people, Sensitive Personal Data must be protected using a combination of the Milestone hardening guide and a general good security practice.

Secondary Personal Data refers to user activity and audit logging. This includes smart client personal user logs including logon/logoff timestamps and audit logging of viewed video streams. Administrative user activities with references to a personal administrator user-id can also be logged with configuration changes, etc.

Is profiling and automated decision-making part of XProtect?

Basic installations of XProtect Corporate do not include any profiling when it comes to GDPR. All automated actions are carried out by the rule engine that can react based on identified events. GDPR compliance in the case of possible action and events handling by the rule engine, depends on the implementation and usage of services used in conjunction with XProtect VMS. For example, installations that use third-party add-on modules such as face recognition and people tracking, are clear cases of profiling with possible action and events handling by the rule engine.

Is XProtect developed using Privacy by Design?

Milestone software is developed using the Milestone Secure Development Lifecycle method. Our current Secure Development Lifecycle guide specifies general security requirements that will soon be extended with our new privacy requirements.

What is an example for an XProtect feature that supports the Privacy by Design approach?

Our Privacy masking feature implemented in 2018 R1 is a great example. By default, only the system administrator can access the system and the 'unmasked' video. New roles added to the VMS will by default have no access to the various functions until otherwise was deliberately configured by an administrator.

Does XProtect provide tools to mask a subject's identity in recorded and live video?

Absolutely. Our Privacy masking feature has both permanent and liftable masks ranging from a light blur to a solid mask. Additional third-party add-on modules can be added for various privacy & security purposes.

Is XProtect developed using Privacy by Default?

Milestone develops its product continuously and Privacy by Default is a key evaluation criterion in XProtect's GDPR-Ready certification. Our Secure development Lifecycle guide is an integral part of Privacy by Default, making sure only the system administrator can access the system in setup and that new roles added to the VMS will by default have no access to the various functions until otherwise was deliberately configured by an administrator.

Does XProtect provide tools to export stored data of a subject using the VMS?

Yes. The function for exporting video is designed for lawful purposes (e.g. exporting forensic material to an officer of the law), and as such, is technically capable of exporting stored data of a subject.

How does XProtect comply with the right to be forgotten?

The right to be forgotten does not often apply to video-surveillance since retention time is usually short and since other lawful basis overrule 'reasonable' technical and legal interests such as legal obligation (employment act), public interest (crime prevention, public health & security), vital interests (life & health critical data, hazardous and dangerous environments), legitimate interests (fraud detection, employment, product development) or even contractual fulfilment (employment, subscriptions and licensing). An

example for a legitimate interest is that video surveillance recordings in most countries must be a trusted source of evidence at any given time, therefore, the VMS primarily protects video evidence from being tampered with and assuring its authentication, making the right to be forgotten secondary.

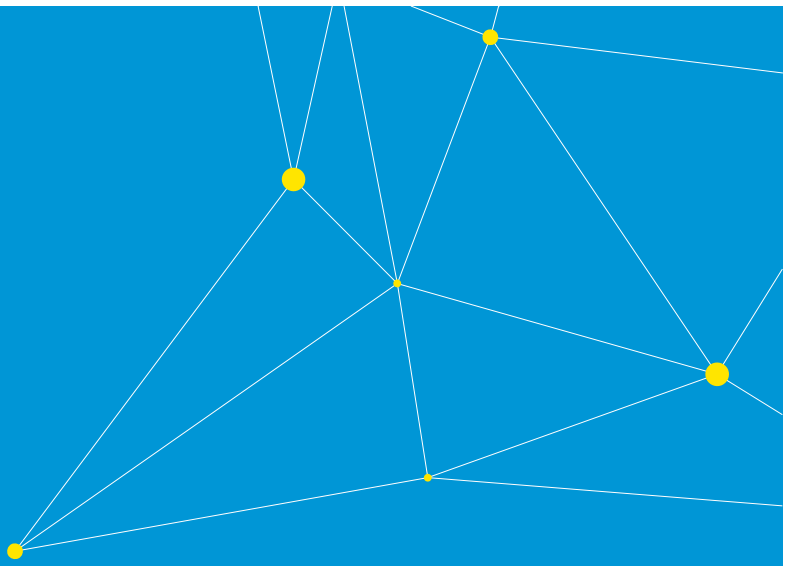
What technical and organizational measures can be taken to protect personal data and to comply with accountability?

The data controller (end-user) must be provided with a documented XProtect installation where access permissions are managed under the least privileged principals and all servers are hardened and operated under best practices (patch & configuration controls). Ideally, the data controller should have a video-surveillance policy in place and an on-the-spot data protection notice listing all the GDPR elements such as purpose and purpose limitations, who has access to live and recorded video, how access permissions are controlled etc. for more information please refer to the EDPS video-surveillance guidelines: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

What security measures does XProtect take to secure personal data?

Our products are designed to deliver end-to-end secure and authenticated video. We use HTTPS to secure the camera connection and recommend setting the cameras on separate VLANs. All video storage is encrypted using AES 256, and we enforce strict authentication and authorization on the server-side. In addition, we make sure all remote access via both our web and mobile clients is encrypted and authenticated for all information exchange. Milestone also recommends that Smart clients and wall boards are on separate VLANs, VPN encrypted network or similar.

Exporting any evidence material is password protected, encrypted and digitally signed, making sure forensic material is genuine, untampered with and viewed by the authorized receiver only. When it comes to user permissions, no default user/password is defined as an administrator until a second administrator is defined as the domain and/or server administrator. Moreover, all new roles/users created will have no access to any functions until otherwise was deliberately configured by an administrator. Administrators are the only ones with access to the audit log which contains the user activity logging. It is also possible to define partial administrator roles to have access only to certain cameras and functions. Our hardening guide is a great way to make sure your installation is setup to the highest level of security.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.