MAKE THE
WORLD SEE

Milestone Systems

GDPR Privacy Guide

milestone

Contents

Copyright, trademarks, and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

GDPR compliance and Milestone XProtect VMS

On May 25th, 2018, the European General Data Protection Regulation (GDPR) came into effect. The objective of this regulation is to give individuals more control over how their personal data is collected, processed and shared.

GDPR provides a structure for businesses that clarifies their roles and responsibilities and gives individuals the opportunity to control how their personal data is used.

This document gives you an overview of the requirements, and how you can work with GDPR compliance when using the XProtect video management system (VMS).

See Appendix: The Milestone XProtect VMS system and GDPR on page 48 for specific information on how a Milestone XProtect VMS system can best be made compliant with GDPR.

Disclaimer: The information in this document and any recommendations are provided as-is. Following this document does not implicitly mean that your system will be GDPR compliant.

The Milestone XProtect VMS requires configuration. Any configuration or modification of settings must comply with EU data protection law. While the Appendix: The Milestone XProtect VMS system and GDPR on page 48 and Additional safeguards on page 51 provide information on how to start a compliant setup, you must adhere to EU data protection laws when further configuring the system.

What is GDPR?

The General Data Protection Regulation (GDPR) is a set of rules that govern all forms of personal data that are held by an organization. GDPR gives every individual ownership of their personal data, and, on the organization's side, introduces accountability at all stages of data processing and storage. GDPR achieves this by providing a number of rights to individuals and putting corresponding obligations on the organizations that process personal data.

GDPR harmonizes data privacy laws across the EU, and it compliments existing national CCTV and video surveillance regulations.

Although GDPR is an EU regulation, it affects many other parts of the world.
It applies to the processing of personal data by a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
It applies to the processing of personal data by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services to data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union.
Furthermore, many other parts of the world are applying similar privacy protection regulations, based on the core principles of GDPR.

GDPR is enforced through domestic authorities.

There are hefty fines in case of violation:

- Up to 4% of the company's world-wide annual revenue
- Up to €20 million per incident

Who is responsible for making sure an XProtect Video Management System complies with GDPR?

The VMS owner is responsible for complying with the GDPR regulation, including:

- Actual installations and the applied usage
- Organizational processes and matureness
- Data breach notification and reporting to authorities

GDPR does not apply to any specific products, but the combination of the product, the data it processes, and the usage of the product and data all affect GDPR compliance.

GDPR has direct implications for installers, system integrators and users of video surveillance technology.

The VMS owner is the Data Controller (see Data Controller on page 12).

The Data Controller might outsource parts or the entire VMS operations to a Data Processor, for example a security company. If this is the case, the Data Controller and the Data Processor must have a Data Processing Contract in place. The Data Processing Contract states what data is processed, how it is protected, and how long the data is kept (see Data Processor on page 19 and Appendix: Data Processing Contract on page 47).

Are all video surveillance installations required to comply with GDPR?

GDPR applies to controllers and processors within the European Union, regardless of where the video is actually processed.

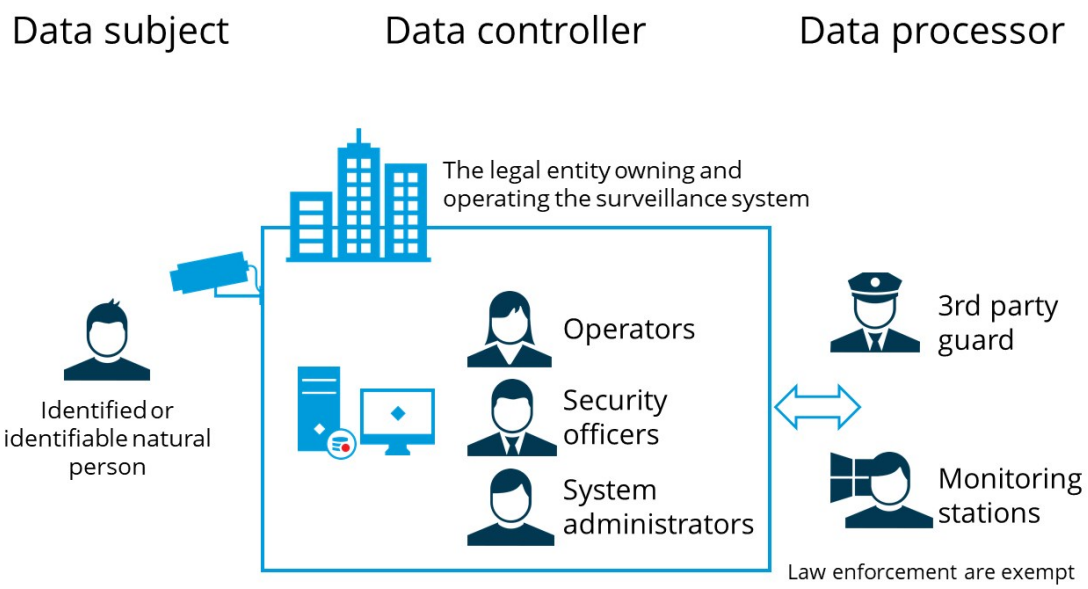
Furthermore, GDPR protects the privacy of any resident of the geographical area of the European Union, covers all forms of video surveillance within the EU, and protects citizens of all countries who reside within the EU (GDPR article 3).

For more information about GDPR, particularly as related to video surveillance, see Appendix: GDPR compliance on page 24.

Who are the key stakeholders of GDPR as related to video surveillance?

When it comes to the GDPR and video surveillance, there are three classes of stakeholder. This section of the document defines each stakeholder and describes their respective responsibilities regarding GDPR.

- Data Subject on page 8
- Data Controller on page 12
- Data Processor on page 19



Data Subject

A Data Subject is any person whose personal data is being collected, held or processed.

Data Subjects are the viewed objects of video surveillance, whether intentional or accidental.

Data Subjects are also any registered person involved in the operation of the VMS, for example, operators or named third-party guards.

The key objective of the GDPR is to safeguard the personal data of these subjects.

Data Subject rights

Articles 12 to 23 of the GDPR cover the rights of the Data Subject.

- Section 1: Transparency and modalities
  - Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
- Section 2: Information and access to personal data
  - Article 13: Information to be provided where personal data are collected from the data subject
  - Article 14: Information to be provided where personal data have not been obtained from the data subject
  - Article 15: Right to access from the data subject (see Right to access on page 30)
- Section 3: Rectification and erasure
  - Article 16: Right to rectification
  - Article 17: Right to be forgotten (Right to erasure) (see Right to be forgotten (Right to erasure) on page 31)
  - Article 18: Right to restriction of processing (see Right to restriction of processing on page 33)
  - Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
  - Article 20: Right to data portability
- Section 4: Right to object and automated individual decision-making
  - Article 21: Right to object
  - Article 22: Automated individual decision-making, including profiling
- Section 5: Restrictions
  - Article 23: Restrictions

Of these, the rights that are most relevant in the context of video surveillance are:

The right to be informed (GDPR Articles 12 to 14 and 34)	Article 12 deals with transparency and modalities, whereas Articles 13 and 14 deal with information and access to personal data. These Articles provide the Data Subject with the ability to be informed of what personal data is collected and how long it is retained. In the VMS context, see Appendix: On-the-spot notice on page 42. Article 34 provides the Data Subject with the right to be informed in case of a data breach if it is likely to result in a high risk to the rights and freedoms of the Data Subject.
The right of access (GDPR Article 15)	This right provides the Data Subject with the ability to get access to his or her personal data that is being processed, for example, video recordings of the data subject. The Data Subject is granted the right to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing.

The right to erasure ("right to be forgotten") (GDPR Article 17)	This right provides the Data Subject with the ability to ask for the deletion of their data. In the VMS context, the erasure upon the Data Subjects' requests are exceptional due to the interests of the controller and the short retention times. (See Appendix: Video surveillance policy on page 43 and *Deleting video recordings partially* in Appendix: The Milestone XProtect VMS system and GDPR on page 48).
The right to object (GDPR Article 21)	This right provides the Data Subject with the ability to object to the processing of their personal data. In the VMS context, other interests such as Legitimate interests (fraud detection, health and safety), Legal obligation (bookkeeping, anti-money laundry) or even contractual fulfillment (employment contracts) may override the interests and rights of the Data Subject. In all cases, this must be fully transparent so the Data Subject can know and object. If the Data Subject objects, the Data Controller must assess the objection, or otherwise he might face a fine.

Data Subject request

Your company must have a process for handling data subject rights requests, for example execute the right of access request. Such a request must be handled within a reasonable time frame. According to Article 12 subparagraph 3 of the GDPR, this is “without undue delay and in any event within one month of receipt of the request.” It is recommended to use the Milestone Data Subject Request example to document such requests, since it may be vital in a GDPR case with national data protection authorities.

The video surveillance policy describes the data subject request (see Appendix: Video surveillance policy on page 43).

What is personal data?

To be compliant with GDPR, you must know what personal data is, and limit the collection of that data to only what is necessary.

According to the regulation, personal data is any information relating to an identified or identifiable person.

An identifiable person is someone who can be identified directly or indirectly, by reference to an identifier such as:

- A name
- An identification number
- Location data
- Online identifier such as IP addresses or cookie identifier
- User data
- Video images
- Or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Personal data is any type of information that directly or indirectly can be used to identify a natural person (Data Subject). This is the data that can be used to identify the viewed objects of video surveillance, whether that data is collected intentionally or accidentally.

Personal data that is protected by GDPR is:

- Data that is processed by the IT product or IT-based service (for example, name and address of a person, video image, payment data, health data).
- Data that is incidentally produced when the product or service is used (for example, usage data, log files, statistical data, data for authorization, configuration data). This data can be personal data of the users of the service, personal data of the people operating the product or service (this may include both staff of the service provider and staff of the users of the product or service), or privacy-relevant configuration data (see Data Controller on page 12).

Personal data is defined as any information relating to an identified or identifiable natural person or Data Subject, for example:

- Full name
- Home address
- Email address
- Phone number
- Location data
- Digital identity
- Vehicle registration plate
- Driver's license number
- Credit card numbers
- Identifiable information, images, etc., such as video recordings and still images
- User activities, such as that found in log files

This data is not necessarily only a direct relation to the object. Personal data can also be a quasi-identifier. Quasi-identifiers are pieces of information that are not of themselves unique identifiers, but are sufficiently well correlated with something so that they can be combined with other quasi-identifiers to create a unique identifier. Quasi-identifiers are particularly important when it comes to special categories of personal data.

Special categories of personal data include data depicting racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation, for example:

- Medical history
- Biometric data (including photos, videos, fingerprints)
- Criminal record
- Racial or ethnic identity
- Genetic information
- Political opinions and engagements
- Religious or philosophical beliefs
- Sexual orientation and history

This is the personal data that potentially is collected by a video surveillance system:

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

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 a video sequence 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.

Special categories of personal data is when the video surveillance is near hospitals (related to health information), jails (criminal convictions), political activity (union membership), religious activity, or images that reveal sexual orientation (for example, gay bars).

Personal data also refers to user data (operator, supervisor, and administrator) activity and audit logging. This includes XProtectSmart Client personal user logs, including log on/log off timestamps and audit logging of accessed video streams, audio or metadata, as well as playback and export of recordings.

See Inherent risks with using VMS on page 46 to make sure that you are not impinging on personal rights.

Data Controller

In the context of video surveillance, Data Controllers own and operate the video surveillance systems. Data Controllers are the legal entity that collects, processes and shares data about the Data Subject.

What are the responsibilities of the Data Controller?

Data Controllers are required to respect data protection principles and fulfill certain specific obligations. The Data Controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. This also includes:

- Applying and maintaining information security policies and procedures to protect personal data. Such internal policies and processes should be approved at the highest level within the organization and therefore be binding for all staff members.
- Maintaining an overview of personal data records and processing flows, for example Record of Processing Activities (Article 30 GDPR) and a list of systems and archives that handle personal data (the XProtect VMS system and other systems that hold personal data such as staff records, data processor agreements, etc., including information on how and where personal data flows).
- Putting in place mechanisms that execute the internal policies and processes, including complaints procedures, in order to make such policies effective in practice. This includes creating data protection awareness, and training and instruction for staff. Awareness training is available at https://www.milestonesys.com/solutions/services/learning-and-performance/.
- Defining the video surveillance policy (see Appendix: Video surveillance policy on page 43). This policy must refer to domestic laws regarding video surveillance.
- Carrying out the Data Protection Impact Assessments, particularly for certain data processing operations deemed to present specific risks to the rights and freedoms of Data Subjects, for example, by virtue of their nature, their scope or their purpose (see Appendix: Data Protection Impact Assessment on page 45).
- Ensuring transparency of these adopted measures with regard to Data Subjects and the public in general. Transparency requirements contribute to the accountability of Data Controllers (for example, publication of privacy policies on the internet, transparency in regard to internal complaints procedures, and publication in annual reports).
- Publishing the right of information notice to the public (see Appendix: On-the-spot notice on page 42). This notice informs individuals who are affected of the purpose of the surveillance, who keeps the data that is collected (Data Controller), and the retention policy.
- Assigning responsibility for data protection to designated persons with direct responsibility for their organizations' compliance with data protection laws. In particular, appoint the Data Protection Officer (DPO).

Data Protection Officer (DPO)

Every organization must have an appointed DPO or at least an assigned person responsible for privacy.

From the start, the plans to install or update a video surveillance system should be communicated to the DPO. The DPO should be consulted in all cases and should be involved in all stages of the decision making.

The DPO's responsibilities include:

- Participating in defining the business purpose of the video surveillance, for example, crime prevention, fraud detection, product quality verification or public health and safety, and so forth.
- Commenting on the organization's draft video surveillance policy, including its attachments, (see Appendix: Video surveillance policy on page 43), and to correcting mistakes and suggesting improvements
- Assisting in communications with the national or regional data protection authorities

- Checking agreements with third-parties when sharing data. That is, maintaining and managing the Data Processing Contract (see Appendix: Data Processing Contract on page 47)
- Drafting compliance reports and carrying out audits in order to obtain third-party certification approving the internal measures adopted to ensure compliance effectively manages, protects, and secures personal data
- Post the Data Breach Notification within 72 hours of being made aware of a breach of security (see Personal data breach on page 19. See also, Milestone Data Breach Notification template).
- Store and make sure that the Record of Processing Activities and Data Protection Impact Assessments (see Appendix: Data Protection Impact Assessment on page 45) are updated every time data protection relevant changes are made to the VMS.

Data Controller roles

The following sections describe the responsibilities of the respective Data Controllers:

- Security officer (VMS supervisor) on page 14
- VMS system administrator on page 16
- VMS operator on page 16

Security officer (VMS supervisor)

Security officers or supervisors are responsible for enforcing the GDPR compliant environment. Security officers must:

- Define user rights (see User rights management on page 14)
- Enforce awareness training of personnel (see Data protection training on page 15)
- Contact the Data Protection Officer (DPO) if GDPR non-compliance is suspected, for example, in the case of data breach of video materials (see Appendix: GDPR compliance on page 24)
- Apply and maintain a high general security level by following the Hardening Guide (see the *Milestone Hardening Guide*)

User rights management

Who should have access to the VMS resources?

Organizations must:

- Limit user access to a small number of clearly identified individuals on a need-to-know basis.
- Maintain audit logs of user access and activities.

Access rights must be limited to a small number of clearly identified individuals on a strictly need-to-know basis. Make sure that authorized users can access only the data to which their access rights refer. Access control policies should be defined following the principle of “least privilege”: access right to users should be granted to only those resources which are strictly necessary to carry out their tasks.

When sharing a computer, Milestone recommends that VMS operators do not share the log in account to Windows. Each operator should have an individual account.

In addition, VMS operators should not select to remember their password when signing in to the VMS system.

Only the security officer, the system administrator, or other staff members specifically appointed by the security officer for this purpose should be able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights must be made in accordance with criteria established in the video surveillance policy (see Appendix: Video surveillance policy on page 43).

Those having access rights must at all times be clearly identifiable individuals. For example, no generic or common user names and passwords should be allocated to an outsourced security company which employs several people to work for the organization.

The video surveillance policy must clearly specify and document the technical architecture of the video surveillance system, who has access to the surveillance video, and for what purpose and what those access rights consist of. In particular, you must specify who has the right to:

- View or access the video in real-time
- Operate the pan-tilt-and-zoom (PTZ) cameras
- View or access the recorded video
- Export recordings and audit trails
- Delete or remove devices (cameras) and delete any recordings
- Alter any data after initial configuration

In addition, you must ensure that only those needing access to the following VMS features get these permissions:

- Administrate the VMS
- Create / edit / view / delete bookmarks
- Create / edit / view / delete evidence locks
- Lift Privacy masks
- Export to defined paths (for example, only export XProtect format with encryption to a shared drive)
- Read audit logs
- Start/stop recording
- Create / edit / delete / activate / lock / release PTZ presets
- Create / edit / delete / start / stop PTZ patrolling schemes
- Audio, metadata, I/O and event permissions

Data protection training

All personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, should be given data protection training and should be familiar with the provisions of GDPR to the extent that they are relevant to their tasks. The training should pay special attention to the need to prevent the disclosure of surveillance video to anyone other than authorized individuals.

Training of personnel is mandatory and must include:

- Cybersecurity
- Export of VMS data

Training should be held when a new system is installed, when significant modifications are made to the system, when a new person joins the organization, as well as periodically afterwards at regular intervals. For existing systems, initial training should be held during the transitory period and periodically afterwards at regular intervals.

See the Milestone GDPR Privacy Guide for VMS Operators and the Milestone GDPR e-learning for VMS Operators.

VMS system administrator

System administrators are responsible for setting up the GDPR compliant system environment. System administrators do amongst the following:

- Apply and maintain a high general security level by following the Hardening Guide (see the *Milestone Hardening Guide*)
- Apply a secure password policy
- Conduct security audits
- Ensure devices record according to the defined purpose – for example, on event, motion, always-on, and so forth
- Ensure recording and audit log retention time is set according to local law and the defined purpose of the VMS
- Ensure user management (add / remove users)
- Ensure cameras follow privacy laws and do not record areas that should not be recorded – mask out areas that should not be recorded
- Contact the Data Protection Officer (DPO) if GDPR non-compliance is suspected, for example, in the case of data breach of video materials (see Appendix: GDPR compliance on page 24)

VMS operator

VMS operators must follow processes and work instructions when accessing data in the system, for example, when viewing video or exporting video, and so forth.

To be GDPR compliant, operators must have the following:

- A general understanding of GDPR and the rules for data export
- Training in GDPR

  Operators should have adequate training of the video surveillance system to ensure that the privacy and other fundamental rights of the subjects caught on the cameras are not intruded upon. They must be taught what the video surveillance policies define (for example, video evidence handout procedures), who to contact if in doubt (escalation point persons such as the supervisor or Data Protection Officer), and so forth (see Data protection training on page 15).

  See also Milestone GDPR Privacy Guide for VMS Operators and the Milestone GDPR e-learning for VMS Operators.

Handling exported data

Exporting is done when there has been an incident that requires sharing evidence with authorities. If you have the rights to export evidence, you have the responsibility when handling it. The reason why it's sensitive is both due to the contents and the fact that the data leaves the surveillance system. Most likely, there has been an incident that may involve criminal activity. There may also be sensitive private details in the evidence. When you export it, it is usually stored on a removable storage of some kind (USB drive, optical disc, etc.).

If that data ends up in the wrong hands, the privacy of the Data Subjects in the evidence would be lost.

You should have a clear process for exporting evidence, which covers:

- Who can export evidence?
- Where is the evidence stored until handed to authorities?
- Who has access to it?
- What format(s) should be used?
- Whether encryption should be applied (highly recommended)?
- When is the evidence destroyed?

Data Controllers must take technical and organizational measures to protect data that leaves the Milestone XProtect VMS. Such measures could be:

- Limit the permission to export videos and audit logs to special personnel only
- Consider encrypting the data before or after it is being exported
- Apply privacy masks before exporting video data, where appropriate
- Physically protect removable media with personal data on it
- Establish policies that ensure that personal data is deleted from media according to the retention time
- Keep a register of removable media – who exported what data to the media? To whom has it been forwarded and for what purpose? Is the recipient informed to destroy the media or to return it after the purpose has been reached? Etc.
- Use Windows group policies to disable USB ports or media access on the client PCs

- Monitor the audit logs for unauthorised export events
- Commit employees to the data protection policy
- Properly sanitize the media or physically delete it if sanitization is not possible (for example, DVDs)

See the Milestone GDPR e-learning for VMS Operators for more information on handling data exports.

Handling exported data in notifications and email

In addition to exports, data can also be extracted from the VMS by means of attachments to notifications. Notifications are emails that are sent to a specified email address. When creating a notification, the administrator can choose to include a set of snapshots or an AVI of a sequence. Because the attached snapshots and AVI sequences in notifications leave the VMS, they are outside the control of the VMS for user access and retention. It is recommended not to attach images or AVI sequences to email notifications. If the attachments are necessary, then you must at least ensure that there are organizational procedures and controls for who receives the emails and how they are handled.

You should have a clear process, which covers:

- Where is the data stored?

  Ensure that the sending and receiving email servers are under control of the organization that is the Data Controller / Data Processor of the video surveillance. In particular, recipients should not be email accounts on free mail accounts such as Gmail or Hotmail, and so forth.

- Who has access to it?
- What format(s) should be used?
- Whether SMTP encryption should be applied?

Please be aware: Use an SMTP/SMTPS mail server. You must encrypt the connection between the VMS and the outgoing mail servers, as well as between the sending and receiving SMTP servers to be covered by the European Privacy Seal. An unencrypted and unsecured connection would violate the EuroPriSe seal and lead to the loss of the EuroPriSe privacy seal compliance.

- When is the data destroyed?

  Milestone recommends that the retention time of video data in the outgoing and incoming mail boxes should be aligned with the retention time of the media database or with the retention time of alarms that may be triggered by the same events that caused the notification.

  Retention time in the mail boxes needs to be limited to a boundary that is reasonable for the purpose behind the notification process.

  Milestone recommends to only use mail boxes of the Data Controller / Data Processor and to configure automatic deletion of the mails after the defined retention time has been reached.

  Data Controllers / Data Processors should make sure that these mail boxes are not automatically archived by the mail system.

Personal data breach

GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of -- or access to -- personal data transmitted, stored or otherwise processed."

In the case of a security breach, the DPO must determine whether to notify the Data Protection Authority and the Data subjects involved, according to Articles 33 and 34 of the GDPR.

According to Article 33 (1) of the GDPR:

> *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

If deemed necessary, the DPO must post the Data Breach Notification within 72 hours of being made aware of the breach (see Milestone Data Breach Notification template). Data Subjects also must be notified if the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals."

Data Processors experiencing a personal data breach must notify the Data Controller, but otherwise have no other notification or reporting obligation under the GDPR.

For information about the other responsibilities of the DPO, see Data Controller on page 12.

Data Processor

If an organization out-sources all or part of its video surveillance activities to a third-party (a Data Processor), it remains liable for compliance with GDPR as a Data Controller. For example, security guards monitoring live surveillance video in the reception area of an organization working for a private company to whom the organization outsourced the task of live monitoring. In this case, the organization must ensure that the security guards carry out their activities in compliance with the GDPR.

To be compliant with GDPR, third-party Data Processors (excluding law enforcement) must:

- Fulfill the same requirements as the operator (see VMS operator on page 16)
- Sign and comply with a Data Processing Contract (see Appendix: Data Processing Contract on page 47).

Summary

GDPR is a regulation that is already influencing how organizations handle data, including video data.

As a minimum, each organization that processes personal data needs one or more designated persons responsible for making sure that the organization handles personal data in line with GDPR and company policy (the number of man hours allocated for this will depend on the size of the organization and the amount of personal data collected and processed). In addition, for some organizations, GDPR will require the appointment of a formal Data Protection Officer (DPO) to perform these tasks.

There will also be changes in the administrative process. Under GDPR, organizations need to keep detailed and accurate Record of Data Processing Activities. There's a range of details that must be recorded, including but not limited to:

- What category of individuals the processed personal data relate to (for example, customers, employees, store visitors, and so forth.)
- For what purposes the personal data is used
- Whether the personal data is going to be transferred – to other companies and/or outside the EU
- How long the personal data will be stored
- Measures taken by the organization, in relation each separate data processing activity, to ensure GDPR compliance

All of this is relevant when it comes to stored surveillance video, and defined in the video surveillance policy (see Appendix: Video surveillance policy on page 43).

Organizations are obligated to explain why a video camera is in a particular place, what is being filmed and why. In the case of video surveillance, appropriate signage in and around the area where the video surveillance is being used should be used to provide information about this.

The Data Controller may be obliged to carry out a Data Protection Impact Assessment (see Appendix: Data Protection Impact Assessment on page 45) when it comes to setting up a camera in a public place. An impact assessment should include:

- A systematic description of the intended processing operations and processing purposes
- An assessment of the necessity and proportionality of the processing operations in terms of purpose (This may require external assistance)
- Risk assessment for individuals' rights and freedoms
- Planned measures to address these risks, including safeguards and mechanisms to ensure the protection of personal data and compliance with GDPR (this should consider the rights and legitimate interests of individuals and other affected persons)

One of the key features of the GDPR is that those who are being monitored need to be fully informed about what data is being held on them and how it's being used. The right of information notice informs individuals who are affected of: the purpose of the surveillance, who keeps the data that is collected (Data Controller / Data Processor), and the retention policy (see Appendix: On-the-spot notice on page 42).

Organizations storing video have clear responsibilities when it comes to storing personal data and must put into place the robust measures to prevent unauthorized access. This means that it's important to set out, in writing, who will have access to the cameras and recordings.

Organizations should also have a procedure in place for when an individual chooses to exercise their right of access to personal data or request its deletion. This is so that they can stay within the prescribed month-long window within which they must comply with these requests under GDPR. When making such a request, it is reasonable to expect the inquirer to provide adequate information to locate this data – for example an approximate time-frame, and the location where the video was captured. That is, the subject should provide official identity papers proving who they are, and the organization should make a record of the recordings being shown or provided to the individual. Furthermore, other people in the video should be masked out, using third-party tools.

Organizations should use strong measures to prevent unauthorized access to the personal data that they are storing. The tactics used by each organization will be unique to the challenges they face. However, in all instances, organizations must employ robust security controls, stay up-to-date with cybersecurity best practice, and ensure that they are working with trusted partners who provide secure hardware, software and thorough aftercare.

Personal data handling

When handling personal data, adhere to these principles:

- Assess: Know what personal information you have in your files and on your computers.
- Reduce: Keep only what you need for your business.
- Protect: Protect the information that you keep.
- Eliminate: Properly dispose of what you no longer need.
- Respond: Immediately report all actual or suspected security breaches.

For more information

- For the full-text version of the *General Data Protection Regulation*
- For information about GDPR for the VMS operator, see *Milestone GDPR Privacy Guide for VMS Operators*
- To stay current and learn more about GDPR developments, visit European Commission website on Data Protection
- For a guide to the GDPR to help organizations comply with its requirements, see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- For a list of key facts about GDPR, see *Key facts on the General Data Protection Regulation*
- For recommendations for European institutions and bodies on how to design and operate video surveillance systems, see the *European Data Protection Supervisor (EDPS) guidelines*
- For information on how to secure your XProtect video management software against cyber-attacks, the see

the *Milestone Hardening Guide*

- For information about how the components of the Milestone XProtect VMS interact, see the *Milestone System Architecture Document*

Milestone GDPR templates

- Milestone Sample On-the-spot notice
- Record of Processing Activities template
- Milestone Video Surveillance Policy template

  You must obey GDPR requirements in setting up and developing the Video Surveillance Policy. Be aware that collecting audio and metadata are not subject of the European Privacy Seal (EuroPriSe).

- Milestone Data Processing Contract template
- Milestone Data Subject Request example

  Note that this is only an example. There are no formal requirements for the requests of Data Subjects.

- Milestone Data Breach Notification template

Appendixes

The following appendixes are provided:

Appendix: GDPR compliance

This section provides an overview of GDPR as regards video surveillance. It describes what GDPR is and how it impacts video surveillance usage in the following sections:

- Do you have a lawful basis for collecting data? on page 24
- Individual rights on page 29
- Privacy by design on page 34
- Accountability on page 40
- Checklist for securing integrity and confidentiality on page 41

Do you have a lawful basis for collecting data?

GDPR requires that all organizations have a valid, lawful basis for collecting and processing personal data.

Video surveillance on the basis of consent or vital interests may be possible in exceptional situations, for example in the health and care if a person has to be monitored permanently.

You are required to keep track of processing activities in a Record of processing activities (Article 30 GDPR).

Check the legitimacy of processing video data and user data in accordance to the following levels of regulation:

1. General Data Protection Regulation (GDPR), Article 6

   Particularly subparagraph 1 (b) of the GDPR:

   *Processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*

   and subparagraph 1 (e)(f) of the GDPR:

> *Processing shall be lawful if and to the extent processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data,* ***in particular where the data subject is a child****.*

2. Directive (EU) 2016/680 Law Enforcement or the national law based on that directive

   Comply with national law based on the Directive (EU) 2016/680 Law Enforcement in order to establish legal basis to check the legitimacy of the processing.

3. National law

   Comply with national law, for example, Section 4 German Federal Data Protection Act (FDPA), though this provision does not apply to video surveillance conducted by enterprises.

Before you implement video surveillance, assess the potential benefits and the impact on the rights to privacy and other fundamental rights and legitimate interests of those in the covered area.

When you decide to use video surveillance, document the purpose of the video system, what information is collected, what it will be used for, by whom, and for how long, and provide adequately supported evidence such as statistical data on the actual number of security incidents that occurred, as well as evidence of past effectiveness of the cameras to deter, prevent, investigate, or prosecute those incidents.

The extent of assessment depends on the size of the proposed system and the impact on people's privacy and other legitimate interests or fundamental rights.

Processing based on legal obligation or on a public task

When is the lawful basis for legal obligations likely to apply? In short, when you are obliged to process the personal data to comply with the law. Article 6 (3) of the GDPR requires that the legal obligation must be laid down by EU law or Member State law.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute. For example, a court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation.

Public institutions usually use video surveillance to perform a public task. Be aware that the balancing of interests is not a legal basis for public authorities in the performance of these tasks.

For public institutions, video surveillance is only legitimate if it is necessary to perform the public task. When performing a public task, you must conduct a proportionality assessment (see Balancing of interests / proportionality assessment). The Data Controller must consider the principles of data minimization (for example, privacy masking), storage limitation (retention time) and purpose limitation (Article 5 (1) GDPR).

Balancing of interests / proportionality assessment

Private bodies usually operate a VMS to pursue legitimate interests of the Data Controller or a third party (Article 6 (1) (f) GDPR). Therefore, a balancing of interests is necessary to check the legitimacy of the processing. The Data Controller needs to identify and weigh his own interests versus the interests or fundamental rights and freedoms of the data subjects, which require protection of personal data.

The processing of audit and alarm history data can usually be based on the legitimate interest of the Data Controller (Article 6 (1) (f) GDPR). The same is applicable for user management data (account data, authentication credentials, authorization data, configuration data) if the user is an employee of a security company.

You must be clear, open and honest with people from the start about how you will use their personal data. In your assessment, address the following questions:

- What are the benefits from using video surveillance? Do the benefits outweigh any detrimental effects?
- Is the purpose of the system clearly specified, explicit and legitimate? Is there a lawful ground for the video surveillance?
- Is the need to use video surveillance clearly demonstrated? Is it an efficient tool to achieve its intended purpose? Are there less intrusive alternatives available?

More so, the Data Controller can only use the personal data for a new purpose if it's compatible with the original purpose, or they get consent, or have a clear basis in law.

Typical interests of the Data Controller

Typically, the Data Controller:

- Exercises the right to determine who shall be allowed or denied access to data
- Safeguards legitimate interests for specifically defined purposes

In the context of employment, the Data Controller should be informed that the processing of employees' personal data – video data as well as user data – in the employment context may be subject to more specific rules under member state law (Article 88 GDPR), for example Section 26 FDPA (Germany).

Typical interests and rights of the data subjects

Data subjects have the right of:

- No long-time surveillance
- No monitoring of intimate situations
- Short retention times
- Adequate safeguards if special categories of personal data (see Art. 9 GDPR) are processed

How XProtect reduces the impact on the interests or fundamental rights and freedoms of the data subject

MilestoneXProtect reduces the impact on the interests and fundamental rights of the data subject by:

- Protection of personal data by:
  - Role-based access control
    - Supervisor only liftable privacy masks
    - Access Logging
  - Encryption of recordings
  - Automated video retention (automated deletion)
  - Privacy masking
  - Secure and verifiable video export
- Cybersecurity
  - System hardening (see the Milestone Hardening Guide)
  - Reporting & patching of known vulnerabilities
- Education and Awareness
  - Partner education certification programs
  - Partner product certification programs (see Milestone Technology Partner Program and Milestone Marketplace)
  - Milestone GDPR e-learning for VMS Operators

Transfers and disclosures

There are three main rules in the GDPR governing transfers, depending on whether the recordings are transferred:

- To a recipient within the organization or in another organization

  In this case, the GDPR provides that the recordings can be transferred to others within the organization or in another organization if this is necessary for the legitimate performance of tasks covered by the competence of the recipient.

- To others within the European Union

  In this case (transfers outside the organizations but within the European Union), these are possible if this is necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or if the recipient otherwise establishes that the transfer is necessary and there is no reason to assume that the legitimate interests of those whose images are transferred might be prejudiced.

- Or to outside the European Union.

  In this case, transfers outside the European Union can be made: (i) if done solely to allow the organization's tasks to be carried out and (ii) only subject to additional requirements, mainly to ensure that the data will be adequately protected abroad.

Summed up

Ensure that you do not do anything with the data in breach of any other laws.

You must use personal data in a fair way. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

You can only use the personal data for a new purpose if it's compatible with your original purpose, or you get consent, or have a clear basis in law.

In some cases that are deemed high risk of encroaching on privacy, you must conduct a formalized impact assessment (see Appendix: Data Protection Impact Assessment on page 45).

Conducting an impact assessment

Before installing and implementing video surveillance systems, you should conduct a privacy and data protection impact assessment.

The purpose of an impact assessment is to determine the impact of the proposed system on individuals' privacy and other fundamental rights, and to identify ways to mitigate or avoid adverse effects.

How much effort should go into the impact assessment? It depends on the circumstances. A video surveillance system with a high risk of encroaching on privacy warrants a greater investment than a video surveillance system with limited impact on privacy, for example, a conventional static CCTV system.

At a minimum, according to Article 35 subparagraph 7 of the GDPR, the assessment must contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Data Controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects referred to in Article 35 (1) of the GDPR:

  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

In any event, and in all cases, you must assess and justify whether to resort to video surveillance, how to place the cameras, select and configure the systems, and how to implement the data protection safeguards defined in this *Privacy Guide* and the Milestone Hardening Guide.

Individual rights

One of the main purposes of GDPR is to give individuals greater protection and a set of rights governing their personal data.

There are some very specific requirements under the terms of the regulation, all of which mean that the party processing or storing personal data has a responsibility to keep this data private.

GDPR gives individuals the right to be made aware when their personal data is being collected (at the point of capture), and how it will be used. In the case of video surveillance, for example, these will mean appropriate signage in and around the area where video surveillance is being used.

Articles 12 to 23 of the GDPR cover the rights of the Data Subject.

- Section 1: Transparency and modalities
    - Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
- Section 2: Information and access to personal data
    - Article 13: Information to be provided where personal data are collected from the data subject
    - Article 14: Information to be provided where personal data have not been obtained from the data subject
    - Article 15: Right to access from the data subject (see Right to access on page 30)
- Section 3: Rectification and erasure
    - Article 16: Right to rectification
    - Article 17: Right to be forgotten (Right to erasure) (see Right to be forgotten (Right to erasure) on page 31)
    - Article 18: Right to restriction of processing (see Right to restriction of processing on page 33)
    - Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
    - Article 20: Right to data portability
- Section 4: Right to object and automated individual decision-making
    - Article 21: Right to object
    - Article 22: Automated individual decision-making, including profiling
- Section 5: Restrictions
    - Article 23: Restrictions

Of these, the rights that are most relevant in the context of video surveillance are:

The right to be informed (GDPR Articles 12 to 14 and 34)	Article 12 deals with transparency and modalities, whereas Articles 13 and 14 deal with information and access to personal data. These Articles provide the Data Subject with the ability to be informed of what personal data is collected and how long it is retained. In the VMS context, see Appendix: On-the-spot notice on page 42. Article 34 provides the Data Subject with the right to be informed in case of a data breach if it is likely to result in a high risk to the rights and freedoms of the Data Subject.
The right of access (GDPR Article 15)	This right provides the Data Subject with the ability to get access to his or her personal data that is being processed, for example, video recordings of the data subject. The Data Subject is granted the right to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing.
The right to erasure ("right to be forgotten") (GDPR Article 17)	This right provides the Data Subject with the ability to ask for the deletion of their data. In the VMS context, the erasure upon the Data Subjects' requests are exceptional due to the interests of the controller and the short retention times. (See Appendix: Video surveillance policy on page 43 and *Deleting video recordings partially* in Appendix: The Milestone XProtect VMS system and GDPR on page 48).
The right to object (GDPR Article 21)	This right provides the Data Subject with the ability to object to the processing of their personal data. In the VMS context, other interests such as Legitimate interests (fraud detection, health and safety), Legal obligation (bookkeeping, anti-money laundry) or even contractual fulfillment (employment contracts) may override the interests and rights of the Data Subject. In all cases, this must be fully transparent so the Data Subject can know and object. If the Data Subject objects, the Data Controller must assess the objection, or otherwise he might face a fine.

For GDPR compliance in VMS systems, three rights are especially relevant: the right to be informed, the right to access, and the right to erasure.

Right to access

Under Article 15, the GDPR gives individuals control over their personal data, including the right to see that data. Particularly important is the right that data subjects can get a copy of their data and that third persons are masked (using third-party tools).

Upon request, organizations need to deliver to a Data Subject all the personal data collected about them, including video collected by a video surveillance system.

Ensure that you establish formal procedures and policies for handling right to access requests, described here in *Register of transfers and disclosures*.

Transfers and disclosures

There are three main rules in the GDPR governing transfers, depending on whether the recordings are transferred:

- To a recipient within the organization or in another organization

  In this case, the GDPR provides that the recordings can be transferred to others within the organization or in another organization if this is necessary for the legitimate performance of tasks covered by the competence of the recipient.

- To others within the European Union

  In this case (transfers outside the organizations but within the European Union), these are possible if this is necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or if the recipient otherwise establishes that the transfer is necessary and there is no reason to assume that the legitimate interests of those whose images are transferred might be prejudiced.

- Or to outside the European Union.

  In this case, transfers outside the European Union can be made: (i) if done solely to allow the organization's tasks to be carried out and (ii) only subject to additional requirements, mainly to ensure that the data will be adequately protected abroad.

Register of transfers and disclosures

The organizations should keep a register—whenever possible, in an electronic form—of transfers and disclosures. In it, each transfer to a third-party should be recorded. (third-parties also include anyone within the organization to whom a transfer is made by those having access to the recordings in the first place. This typically includes any transfer outside the security unit.) The register, in addition, should contain all instances where, although the copy of the video surveillance recording was not transferred, third-parties were shown the recordings or when the content of the recordings was otherwise disclosed to third-parties.

The register should include at least the following:

- Date of the recordings
- Requesting party (name, title and organization)
- Name and title of the person authorizing the transfer
- Brief description of the content of the recordings
- Reason for the request and the reason for granting it
- Whether a copy of the recording was transferred, the recording was shown, or verbal information was given

Right to be forgotten (Right to erasure)

Under Article 17, the GDPR gives individuals control over their personal data, including the right to have their personal data erased if it is no longer necessary for the intended purpose of the system.

According to Article 17 subparagraph 1c of the GDPR, the Data Controller must handle objections of data subjects. Since deleting a specific subject from video is not practical, data-processors should strictly limit how long video is retained in accordance with the documented purpose of the system.

What should you do?

Review retention time for all cameras, and ensure it is set in accordance with the documented system purpose.

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 fulfillment (employment, subscriptions and licensing). An example for a legitimate interest is that video surveillance recordings 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.

There are usually two reasons for data subjects to object the storage of video recordings:

- The interests of the Data Controller to store the data are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (Article 17 subparagraph 1c GDPR)
- The personal data have been unlawfully processed, for example the surveillance of a kindergarten or a locker room (Article 17 subparagraph 1d GDPR)

Therefore, each request must be examined thoroughly.

How long should the recordings be kept?

The general principle is that recordings must not be retained longer than necessary for the specific purposes for which they were made. It must also be considered whether recording is necessary in the first place and whether live monitoring without recording would be enough.

If an organization opts for recording, it must specify the period for which the recordings will be retained. After the lapse of this period the recordings must be erased. Milestone XProtect VMS automates the process of erasure, by automatically deleting recordings older than the set retention time.

When files containing the recorded video data are deleted by the VMS, the files and their content are actually not erased from the data blocks on the storage system but simply marked as free in the file system, allowing other files to be written to this location on the storage system. Until the data blocks are actually overwritten with new data, the old deleted video data may potentially be restored, providing access to recordings older than the set retention time.

Because of this it is recommended not to over dimension the storage system, because the risk becomes larger with the size of the overhead.

For example, if the allocated storage system is twice as large as the amount of video data stored for the set retention time – for example seven days - the deleted data blocks containing old deleted video data may statistically lurk around on the storage system for an additional seven days before they are overwritten.

To further reduce the risk of accessing old video data that has been deleted, and for security in general, it is recommended to enable encryption of the media databases, because this, in addition to restoring the delete files, now also requires the encryption to be broken.

Regardless if the video data has been encrypted or not, once the disks in the storage system are no longer useable, it important that you sanitize or physically destroy the hard disks that have been used to store media databases before you dispose of them (for example, by shredding or other equivalent means).

For information about how to set this up in Milestone XProtect, see "Storage and archiving (explained)" in the *XProtect VMS Products - Administrator manual*.

If the purpose of the video surveillance is security, and a security incident occurs and it is determined that the recordings are necessary to further investigate the incident or use the recordings as evidence, the relevant recording may be retained beyond the normal retention periods for as long as it is necessary for these purposes. Thereafter, however, they must also be erased.

Retention period for typical security purposes: one week to one month

When cameras are installed for purposes of security, one week to one month should be enough time for security personnel to make an informed decision whether to retain a recording for a longer period to further investigate a security incident or use it as evidence.

An example of local law: according to some German Data Protection Authorities and most of the data protection literature, this retention period is from 48 to 72 hours as a guideline for the purposes of access control and investigation of criminal offenses.

Member State or third country territory: 48 hours

In case the surveillance covers any area outside the buildings on Member State (or third-country) territory (typically those near entrance and exit areas) and it is not possible to avoid that passers-by or passing cars are caught on the cameras, it is recommended to reduce the retention period to 48 hours or otherwise accommodate local concerns whenever possible.

Right to restriction of processing

The Data Subject may, with reference to Article 18.1 of the GDPR, claim the right to restriction of processing. In a basic VMS scenario, the Data Subject may claim that the VMS processing is unlawful, for example if the Data Subject is unaware that video surveillance of a public space is performed with privacy mask protection. It is recommended to use the Data Subject Request example to document the claim (see Data Subject request on page 10).

The claim should be processed within a reasonable time-frame, faster than the retention period to avoid automated retention or deletion of the VMS evidence in the claim. It is generally advised to seek legal counsel concerning restriction of processing. One way to handle such a request is to let the VMS Administrator limit VMS Supervisors or Operators by role assignment to only be able to playback recordings within a short time after they have been recorded – for instance, four hours or one day (see What should you do? on page 34: "Consider

restricting access to recorded video for operators, either completely, to only the video recorded in the past few hours, or only with dual authorization"). Limitations of playback also apply to evidence locks. If further restrictions of processing are required, it is recommended to conduct both a business impact assessment and a Privacy Impact Assessment (see Conducting an impact assessment on page 28) as part of the claim handling.

Privacy by design

The GDPR mandates that privacy must be a priority throughout system design and commissioning. The approach taken with respect to data privacy must be proactive, not reactive. Risks should be anticipated, and the objective must be to prevent events before they occur.

Organizations must carefully consider and document how systems are designed to stay within the stated objectives.

Care must be paid not to capture personal data of subjects who fall outside of the domain of the system (for example, adjacent public areas).

Careful consideration of who needs to see what information (for example, live/recorded, time frame, resolution) and who can access what features (for example, search).

What should you do?

- Document the resolution of different points in the camera scene
- Document the intended retention time
- Consider applying privacy masking – permanent or liftable
- Consider setting up permissions for viewing live videos, recordings
- Consider restricting access for exporting recordings and for lifting privacy masks
- Regularly review roles and responsibilities for operators, investigators, system administrators and others with access to the system
- Consider restricting access to groups tasked with investigations for cameras that are specifically positioned to capture identity (for example, faces of people entering a store)
- Consider restricting access to recorded video for operators, either completely, to only the video recorded in the past few hours, or only with dual authorization
- Limit the number of users who have an Administrator Role

Requirements for privacy by design

Data minimization	You must ensure the personal data you are processing is: • adequate – enough to properly fulfill your stated purpose • relevant – has a rational link to that purpose • limited to what is necessary – you do not hold more than you need for that purpose.

Accuracy	Generally, for personal data: • You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact. • You may need to keep the personal data updated, although this will depend on what you are using it for. • If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible. • You must carefully consider any challenges to the accuracy of personal data.
Storage period limitation	• You must not keep personal data for longer than you need it. • You need to think about—and be able to justify—how long you keep personal data. This will depend on your purposes for holding the data. • You need a policy that sets standard retention periods wherever possible, to comply with documented requirements. • You should also periodically review the data you hold, and erase or anonymize it when you no longer need it. • You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data. • You may keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Privacy by design and privacy by default

According to GDPR, the controller of personal data, when processing such data, has an obligation to implement technical or organizational measures which are designed to implement the data protection principles set out in GDPR. GDPR refers to this as privacy by design.

In the context of a camera, a relevant example of privacy by design would be a feature that digitally allows the user to restrict image capture to a certain perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured.

In the XProtect VMS, there is support for privacy masking in two forms: permanent masks that cannot be removed, and liftable masks that (with the right permissions) can be lifted to reveal the image behind the mask.

The Data Controller also has an obligation to implement technical or organizational measures which by default ensure the least privacy intrusive processing of the personal data in question. GDPR refers to this as privacy by default. In the context of a camera, a relevant example of privacy by default could be using privacy masking to keep a sensitive area within the view of the camera private.

What is an example for an XProtect feature that supports the privacy by design approach?

Milestone develops its portfolio of products continuously, and privacy by default is a key evaluation criterion in making XProtect GDPR compliant. The Milestone Secure Development Lifecycle guide is an integral part of privacy by default, applying principles such as "defense in depth," "least privileges," and avoiding less secure default settings and turning off infrequently used features by default.

What should you do to ensure privacy by design?

- Consider the resolution of different points in the camera scene and document these settings

  Different purposes require different image qualities. When identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognizable facial images are captured.

- Encrypt your recordings

  Milestone recommends that you secure your recordings by enabling at least Light encryption on your recording servers' storage and archives. Milestone uses the AES-256 algorithm for encryption. When you select Light encryption, only a part of the recording is encrypted. When you select Strong encryption, the entire recording is encrypted.

- Secure the network

  Milestone recommends that you select cameras that support HTTPS. It is recommended that you set the cameras on separate VLANs and use HTTPS for your camera to recording server communication, as well as clients to recording server communication.

  It is recommended that you enable encryption of the media communication from the Recording Server to other servers and clients.

  It is recommended that XProtect Smart Clients and XProtect smart walls are on the same VLAN as the servers.

  Use a VPN encrypted network or similar if using Smart Client or Smart Wall from a remote location.

- Enable and document the intended retention time

  According to Article 17 subparagraph 1a of the GDPR, recordings must not be retained longer than necessary for the specific purposes for which they were made. Milestone recommends that you set the retention time appropriately. This, then, automates the disposal of video.

- Secure exports

  Milestone recommends that you only allow access to export functionality for a select set of users that need this permission.

  Milestone also recommends that the Smart Client profile is changed to only allow export in XProtect Format with encryption enabled. AVI and JPEG exports should not be allowed, because they can not be made secure. This makes export of any evidence material password protected, encrypted and digitally signed, making sure forensic material is genuine, untampered with and viewed by the authorized receiver only.

- Enable privacy masking – permanent or liftable

  Use privacy masking to help eliminate surveillance of areas irrelevant to your surveillance target.

- Restrict access rights with roles

  Apply the principle of least privilege (PoLP).

  Milestone recommends that you only allow access to functionality for a select set of users that need this permission. By default, only the system administrator can access the system and perform tasks. All new roles and users that are created have no access to any functions until they are deliberately configured by an administrator.

  Set up permissions for all functionality, including: viewing live video and recordings, listening to audio, accessing metadata, controlling PTZ cameras, accessing and configuring Smart Wall, lifting privacy masks, working with exports, saving snapshots, and so on.

  Restrict access to recorded video, audio, and metadata for operators, either completely, or restrict access to only the video, audio, or metadata recorded in the past few hours or less.

  Regularly assess and review roles and responsibilities for operators, investigators, system administrators and others with access to the system. Does the principle of least privilege still apply?

- Enable and use two-step verification

  Milestone recommends that you specify an additional login step for users of XProtect Mobile or XProtect Web Client by enabling two-step verification.

- Restrict administrator permissions

  Milestone recommends that you limit the number of users that have an Administrator Role.

Setting up and configuring the video surveillance system

The guiding principle in connection with all items addressed in this section should be to minimize any negative impact on the privacy and other fundamental rights and legitimate interests of those under surveillance.

Camera locations and viewing angles

Camera locations should be chosen to minimize viewing areas that are not relevant for the intended purposes.

As a rule, where a video surveillance system is installed to protect the assets (property or information) of the organization, or the safety of staff and visitors, the organization should restrict monitoring to

- carefully selected areas containing sensitive information, high-value items or other assets requiring heightened protection for a specific reason,
- entry and exit points to the buildings (including emergency exits and fire exits and walls or fences surrounding the building or property), and
- entry and exit points within the building connecting different areas which are subject to different access rights and separated by locked doors or another access control mechanism.

Number of cameras

The number of cameras to be installed will depend on the size of the buildings and the security needs, which, in turn, are contingent upon a variety of factors. The same number and type of cameras may be appropriate for one organization and may be grossly disproportionate for another. However, all other things being equal, the number of cameras is a good indicator of the complexity and size of a surveillance system and may suggest increased risks to privacy and other fundamental rights. As the number of cameras increases, there is also an increased likelihood that they will not be used efficiently, and information overload occurs. Therefore, the European Data Protection Supervisor (EDPS) recommends limiting the number of cameras to what is strictly necessary to achieve the purposes of the system. The number of cameras must be included in the video surveillance policy.

Times of monitoring

The time when the cameras are set to record should be chosen to minimize monitoring at times that are not relevant for the intended purposes. If the purpose of video surveillance is security, whenever possible, the system should be set to record only during times when there is a higher likelihood that the purported security problems occur.

Resolution and image quality

Adequate resolution and image quality should be chosen. Different purposes will require different image qualities. For example, when identification of the individuals is crucial, the resolution of the cameras, compression settings in a digital system, the location, the lighting and other factors should all be considered and chosen or modified so that the resulting image quality would be sufficient to provide recognizable facial images. If identification is not necessary, the camera resolution and other modifiable factors can be chosen to ensure that no recognizable facial images are captured.

Who should have access to the VMS?

Access rights must be limited to a small number of clearly identified individuals on a strictly need-to-access basis. VMS access policies should be defined following the principle of “least privilege”: access right to users should be granted to only those resources which are strictly necessary to carry out their tasks.

Only the Data Controller, the system administrator, or other staff members specifically appointed by the Data Controller for this purpose should be able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights must be made in accordance with criteria established in the organization's video surveillance policy.

Those having access rights must always be clearly identifiable individuals.

The video surveillance policy must clearly specify and document who has access to the video surveillance recordings and/or the technical architecture, for example VMS servers, of the video surveillance system, for what purpose and what those access rights consist of. In particular, you must specify who has the right to

- View the video/audio in real-time
- Operate the pan-tilt-and-zoom (PTZ) cameras
- View the recordings
- Export, or
- Delete any recording

In addition, you must configure access to the following VMS features:

- Bookmarks
- Evidence locks
- Lift Privacy masks
- Export
- Trigger events
- Start/stop recording
- Create/edit/delete/activate/lock/release PTZ presets
- Create/edit/delete/start/stop PTZ patrolling schemes
- Smart Search
- Audio, metadata, I/O and event permissions

Protecting stored and transmitted data

First and foremost, an internal analysis of the security risks must be carried out to determine what security measures are necessary to protect the video surveillance system, including the personal data it processes.

In all cases, measures must be taken to ensure security with respect to

- Transmission
- Storage (such as in computer databases)
- Access (such as access to servers, storage systems, the network, and premises)

Transmission must be routed through secure communication channels and protected against interception, for example by means of:

- Encryption of the media from the Recording Server to the servers and clients
- HTTPS camera to the Recording Server
- VPN for Smart Client or Management Client connected via internet
- HTTPS for Web and Mobile client

Protection against interception is especially important if a wireless transmission system is used or if any data is transferred via the internet. In these cases, the data must be encrypted while in transit or equivalent protection must be provided.

Encryption or other technical means ensuring equivalent protection must also be considered in other cases, while in storage, if the internal analysis of the security risks justifies it. This may be the case, for example, if the data is particularly sensitive. This is done by enabling encryption of the media database.

All premises where the video surveillance data is stored and where it is viewed must be secured. Physical access to the control room and the server room where the VMS servers are placed must be protected. No third-parties (e.g. cleaning or maintenance personnel) should have unsupervised access to these premises.

The location of monitors must be chosen so that unauthorized personnel cannot view them. If they must be near the public areas, the monitors must be positioned so that only the security personnel can view them.

The XProtect VMS logs basic information by default, but we recommend that you enable user access logging in the Management Client for the audit log.

This digital logging system is in place to ensure that an audit can determine at any time who accessed the system, where and when. The logging system can identify who viewed, deleted, or exported any video surveillance data (this requires that you enable user access logging, as described in the *Milestone Administrator Manual*). In this respect, and elsewhere, attention must be paid to the key functions and powers of the system administrators, and the need to balance these with adequate monitoring and safeguards.

Accountability

Article 5 (2) of the GDPR states:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Where the principles relating to processing of personal data are: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.

The accountability principle requires you to take responsibility for what you do with personal data.

More specifically, Article 30 of the GDP states:

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

The record must contain all of the following information:

a. *the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer*

b. *the purposes of the processing*

c. *a description of the categories of data subjects and of the categories of personal data*

d. *the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations*

e. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards

f. where possible, the envisaged time limits for erasure of the different categories of data

g. where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.

You need to put in place appropriate technical and organizational measures to meet the requirements of accountability.

There are several measures that you can take, and in some cases must take, including:

- Adopting and implementing data protection policies
- Taking a 'data protection by design and default' approach (for more information, see Privacy by design on page 34)
- Putting written contracts in place with organizations that process personal data on your behalf
- Maintaining documentation of your processing activities
- Implementing appropriate security measures
- Recording and, where necessary, reporting personal data breaches
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- Appointing a data protection officer
- Adhering to relevant codes of conduct and signing up to certification schemes

Use the Record of Processing Activities template to identify and track accountability issues.

Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.

If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organization.

Being accountable can help you to build trust with individuals and may help you mitigate GDPR enforcement action.

Checklist for securing integrity and confidentiality

The GDPR requires organizations have comprehensive policies and procedures ensuring personal data always remains within control of the organization. Additionally, personal data breaches must be reported within 72 hours to the competent supervisory authority appointed by their country's government.

Take all appropriate organizational and technical measures to protect against compromising personal data.

What should you do?

- Review security policies around password control and account use.
- Consider setting minimum password strength requirements for all domain groups. Consider setting stronger requirements for administrative accounts on the domain level.
- Have processes in place to audit protection status and detect breaches.
- Ensure users do not share accounts, whether by sharing passwords or by not logging off/on at the end/start of their shift.
- Maintain a documented policy and procedure governing appropriate actions in the event of data breach.
- You must ensure that you have appropriate security measures in place to protect the personal data you hold.
- A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organizational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organizational policies, and physical and technical measures.
- You must also take into account additional requirements about the security of your processing – and these also apply to Data Processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymization (for example, using privacy protection with a blurring mask), and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures and undertake any required improvements.

Appendix: On-the-spot notice

On-the-spot notices should include a pictogram (for example, the ISO pictogram or the pictogram customarily used where the building is located. It is important that the pictogram is also understandable for children. You can find this, for example, on the ISO graphical symbols page (https://www.iso.org/obp/ui/#search/grs/). The notice must:

- Identify the Data Controller
- Specify the purpose of the surveillance:
    - For public bodies to perform their tasks
    - To exercise the right to determine who shall be allowed or denied access
    - To safeguard legitimate interests for specifically defined purposes
- Clearly mention if the images are recorded
- Provide contact information and a link to the online video surveillance policy
- If any area outside the buildings is under surveillance, this should be clearly stated

Security staff and reception must be trained on the data protection aspects of video surveillance practices and must be able to make copies of the detailed data protection notice (see Appendix: Video surveillance policy on page 43), available upon request. They must also be able to tell members of the public whom to contact with additional questions or to access their data.

The signs must be placed at such locations and be large enough that Data Subjects can notice them before entering the monitored zone and can read them without difficulty. This does not mean that a notice must be placed next to every single camera.

The signs within the buildings must be in the language (or languages) generally understood by staff members and most frequent visitors. Signs outside the buildings (if any areas outside are monitored) must also be posted in the local language (or languages).

For an example of an On-the-spot notice, see the Milestone Sample On-the-spot notice.

Appendix: Video surveillance policy

The video surveillance policy has many purposes and serves to meet the following needs:

- Adopting this document is often necessary to complete and specify the legal basis and thus, help establish a lawful ground for the video surveillance (see Article 5 of the GDPR).
- Putting practices in writing and thinking through what other additional measures need to be taken are likely to improve procedures and ensure better compliance.
- Adopting a policy and making it publicly available will help fulfill the obligation under the GDPR to provide the public with the information necessary to guarantee fair processing.
- The policy establishes a set of rules against which compliance can be measured (for example, during an audit).
- By increasing transparency and demonstrating compliance efforts, organizations induce trust in their employees and in third-parties, and help facilitate consultation with stakeholders.

The video surveillance policy should provide the following:

- Give an overview of the video surveillance system and describe its purposes
- Describe how the system is operated, personal data are used, and what data protection safeguards are put in place
- Explicitly confirm compliance with GDPR
- Outline any necessary measures required for implementation

Organizations should make their video surveillance policies publicly available on their intranet and internet sites. If this document contains confidential information, then a non-confidential version should be made publicly available.

To be able to serve as an adequate data protection notice, the following information must be integrated into your video surveillance policy in user-friendly language and format:

- Identity of the Data Controller (for example, organization, Directorate General, Directorate and unit)
- Brief description of the coverage of the video surveillance system (for example, entry and exit points, computer rooms, archive rooms)
- The legal basis of the video surveillance, for example Article 6 subparagraph 1 (f) of the GDPR
- The data collected and the purpose of the video surveillance (any limitations on the permissible uses should also be clearly specified)
- Who has access to the surveillance material, and to whom the recordings may be disclosed
- How the information is protected and safeguarded
- How long the data is kept
- How Data Subjects can verify, modify or delete their information (including contact information for further questions and information on how to obtain recourse in-house)

In addition, the video surveillance policy should provide references to:

- The organization's audit reports
- The organization's impact assessment reports

For a sample template of a Video Surveillance Policy, see the Milestone Video Surveillance Policy template.

Disclaimer: The sample Video Surveillance Policy must be checked by the Controller. GDPR compliance using this sample is his area of responsibility.

Please be aware: collecting audio and meta data is not covered by the European Privacy Seal. A VMS configuration with the collection of audio and meta data is not entitled to use the EuroPriSe certified product profile. A controller / processor doing so cannot point out that he or she is using a product which especially facilitates data protection and GDPR compliance.

Appendix: Data Protection Impact Assessment

According to Article 35 of the GDPR, a Data Protection Impact Assessment is required if the surveillance

is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The Data Controller must consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk (Prior Consultation, Article 36 of the GDPR).

Create and maintain an impact assessment, a notice to individuals affected. This document:

- Describes the purpose of surveillance
- Is kept by the Data Controller or Data Processor
- Defines the retention policy

A privacy and data protection impact assessment should be carried out before installing and implementing video surveillance systems whenever this adds value to the organization's compliance efforts. The purpose of the impact assessment is to determine the impact of the proposed system on individuals' privacy and other fundamental rights and to identify ways to mitigate or avoid any adverse effects.

At a minimum, according to Article 35 subparagraph 7 of the GDPR, the assessment must contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Data Controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects referred to in Article 35 (1) of the GDPR:

  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

The effort that is appropriate to invest in an impact assessment depends on the circumstances. A video surveillance system with large inherent risks, or one raising complex or novel issues, warrants investment of much more effort than one with a comparatively limited impact on privacy and other fundamental rights, such as a conventional static CCTV system operated for typical security purposes.

In any event and in all cases, whether in a formal impact assessment or otherwise, the organizations must assess and justify whether to resort to video surveillance, how to site, select and configure their systems, and how to implement the data protection safeguards.

In addition, there may be cases where an organization proposes a non-standard system. In this case the organization should carefully assess the planned differences from the practice and recommendations, discuss these with their DPO and with other stakeholders, and document its assessment in writing, whether in a formal impact assessment or otherwise. The organization's audit of the system should also address the lawfulness of the customization of the system.

Finally, due to their complexity, novelty, specificity, or inherent risks, it is strongly recommended that you carry out an impact assessment in the following cases:

- Video surveillance for purposes other than security (including for investigative purposes)
- Video surveillance of public spaces
- Employee monitoring
- Monitoring on Member State territory and in third countries
- Special categories of data
- Areas under heightened expectations of privacy
- High-tech and/or intelligent video surveillance
- Interconnected systems
- Audio recording

The impact assessment may be carried out in-house or by an independent contractor. The assessment should be conducted at an early stage of the project. Based on the results of the impact assessment an organization may decide:

- To refrain from or modify the planned monitoring and/or
- To implement additional safeguards

Inherent risks with using VMS

When maintaining the Data Protection impact Assessment, you should be aware of the risks that are inherent with using VMS.

The impact assessment should be adequately documented. As a matter of principle, an impact assessment report should clearly specify the risks to privacy and/or other fundamental rights that the organization identified, and the additional safeguards proposed. Be aware of the following risks of impinging on personal rights:

- Company / employer, using the video feeds, alarms or audit logs to:
  - Monitor the work hours of the employees at the surveyed site – for example arrival and departure time
  - Monitor the effectiveness of the employees by monitoring where they spend their time, amount of time spent at coffee machine, time spent in restrooms, as long as they effectively work at whichever task they have
  - Monitor what the employee is looking at on their computer screens
  - Monitor if employees comply with work or safety requirements – for example on building sites
  - Show video recordings of employees to other employees or managers in order to bully the employee or threaten other employees to do the same
  - Check if security guards / operators perform their duties effectively – for example checking whether they are actively using the clients, selecting cameras, running playbacks, etc.
- Company / owner / operator / guards, using the video feeds to:
  - Share video recordings of people (company employees or the general public) in embarrassing or sensitive situations on social media
  - Use PTZ cameras to zoom in on people to get intimate / inappropriate close-up recordings of them without their knowledge
- Company / owner / operator / guards
  - Export video or providing access to recorded video uncritically to whomever asks for it

Additional sources to identify risk are:

- The *Milestone Hardening Guide* provides the Cyber Risk Management Framework, describing the recommended six steps of categorizing, selecting, implementing, assessing, authorizing, and monitoring risks. The *Hardening Guide* provides a series of technical risks and recommended implementations to mitigate the risks. These include but are not limited to the protection of VMS privacy in terms of s series of data breach and unauthorized access risks from weak technical configuration, design and maintenance operations.
- The *Milestone Privacy Guide* (this) provides recommendations on handling the non-technical operational risks, including handling of data subject rights and requests, roles and responsibilities of a VMS, templates for on-the-spot-notice, video surveillance policy and Data Processor Agreements.
- The Milestone end-user privacy e-learning provides awareness training for VMS operations and supervisors on how, in everyday operation, to handle VMS related privacy risks. See on the Milestone Systems web site.

Appendix: Data Processing Contract

The Data Controller must have a Data Processing Contract with any third-party with whom the Data Controller shares video surveillance media with, with the exception of sharing video surveillance media with law enforcement.

If an organization outsources all or part of its video surveillance activities to a third-party (a Data Processor), it remains liable for compliance with GDPR as a Data Controller. For example, security guards monitoring live surveillance video in the reception area of an organization working for a private company to whom the organization outsourced the task of live monitoring. In this case, the organization must ensure that the security guards carry out their activities in compliance with the provisions GDPR.

For a sample template of a Data Processing Contract, see the Milestone Data Processing Contract template.

Disclaimer: The sample Data Processing Contract must be checked by the Controller. GDPR compliance using this sample is his area of responsibility.

Appendix: The Milestone XProtect VMS system and GDPR

Please be aware: This section describes requirements and restrictions to be a European Privacy Seal (EuroPriSe) certified product. A controller / processor deviating from these requirements cannot point out that he or she is using a product which especially facilitates data protection and GDPR compliance.

Components and devices that are not covered by the European Privacy Seal

The following components are not covered by the European Privacy Seal:

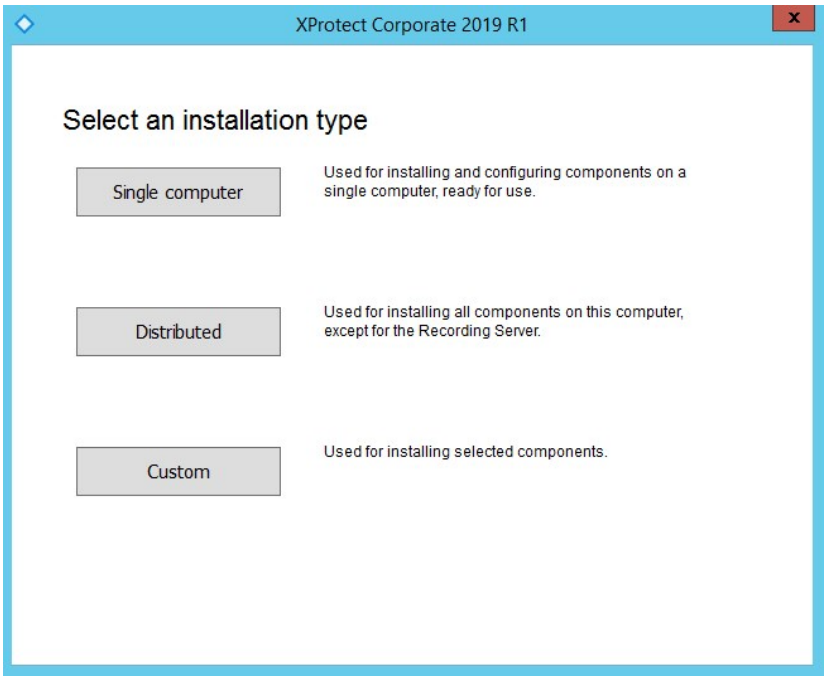
- Mobile Server (disabled by default)
- XProtect® Mobile client
- XProtect Web Client
- XProtect Access (disabled by default)
- XProtect LPR (disabled by default)
- XProtect Transact (disabled by default)
- XProtect DLNA Server
- Milestone ONVIF Bridge (secure private-to-public video integration)
- Event Server Plug-ins
- Milestone Interconnect
- Audio, Input and Output (I/O) Devices, and metadata (disabled by default)

For the Milestone XProtect VMS installation to be covered by the European Privacy Seal, these components must not be installed.

In addition, the standard product does not perform facial recognition, behavior analysis, automatic tracking or recognition of persons in the live feed or the recorded media. This functionality is also not compliant with the European Privacy Seal.

This means that when you install the XProtect VMS, do not use the **Single computer** option in the installer, because this automatically installs the Mobile Server.

Instead, install the XProtect VMS system with either the **Distributed** or **Custom** options. These do not install the Mobile Server.



After the XProtect VMS has been installed, the download page on the Management Server will list the additional XProtect DLNA Server and Mobile Server components. Do not install these servers.

Create Users

Do not create basic user types. If you add basic users to your system, the system will not be compliant with the GDPR legislation.

Milestone recommends that you delete all basic users and create these users as Windows Active Directory type users.

Please be aware: Using the basic user type is not covered by the European Privacy Seal. A VMS configuration with basic user type is not entitled to use the EuroPriSe certified product profile. A controller / processor doing so cannot point out that he or she is using a product which especially facilitates data protection and GDPR compliance.

XProtect relies on Windows mechanisms for authentication and favors a domain controller for user and security management. It is then consistent to delegate the definition of security policies and their enforcement to an Active Directory. This way an enterprise can consistently manage their security and access control policies in one central place. Customers do not have to duplicate security policies in XProtect and keep adjustments manually in sync.

In a workgroup environment, all relevant security policies for Windows accounts are locally administered and enforced on the Windows machine that hosts the Management Server.

Refer to the *Milestone Hardening Guide* for more information.

Upgrade guide

If you are upgrading a Milestone XProtect VMS installation version 2018 R2 or earlier, the old logs must be deleted manually for the installation to be GDPR compliant.

After you have upgraded the XProtect VMS, the old logs can be deleted using the information and the tool described in this Knowledge Base article.

Secure network for authentication and data transmission

Design a network infrastructure that uses physical network or VLAN segmentation as much as possible.

Milestone recommends that you select cameras that support HTTPS. It is recommended that you set the cameras on separate VLANs and use HTTPS for your camera to recording server communication, as well as clients to recording server communication.

It is recommended that XProtect Smart Client and XProtect Smart Wall are on the same VLAN as the servers.

Use a VPN encrypted network or similar if using Smart Client or Smart Wall from a remote location.

Refer to the *Milestone Hardening Guide* for more information.

Please be aware: Unencrypted and unsecured transport of video data would violate the EuroPriSe seal and lead to the loss of the EuroPriSe privacy seal compliance.

Masking individuals in the case of access

According to GDPR Article 15, the Data Subject has the right to get access to his or her personal data that is being processed, for example, video recordings of the Data Subject.

The Data Subject is granted the right to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing.

Because XProtect VMS does not support automatic identification of individuals, you must put in place additional measures to safeguard the individuals' rights. In the VMS context, see Appendix: On-the-spot notice on page 42.

More so, XProtect VMS does not support the masking of other persons who are moving who are recorded together with the claimant for the right of access.

Several Milestone technical partner solutions for dynamic blurring of all or other persons before export can be found on Milestone Marketplace. Alternatively blurring can be added to single images or video streams either manually or assisted after export. Some companies offers blurring as a service (for example, FACIT Data Systems).

Deleting video recordings partially

According to GDPR Article 17, the Data Subject has the right to ask for the deletion of their data. In the VMS context, this is often not fulfilled due to overriding legitimate interests (fraud detection, health and safety) or other business purposes stated in the Video surveillance policy (see Right to be forgotten (Right to erasure) on page 31 and Appendix: Video surveillance policy on page 43). The Video surveillance policy defines the automatic retention (default 7 days) that ensures automatic deletion of footage, and this must fairly balance data subjects rights against reasonable business purposes.

If a Data Subject requests their data to be deleted, it is recommended that the Data Controller uses the Data Subject Request example to document the claim (see Data Subject request on page 10).

You must delete all recordings from the camera or cameras in question.

To retain all the other recordings that should not be deleted, export all of the data and keep it secure. You cannot restore this data back to the VMS.

Any export must be encrypted and digitally signed, and exclude the specified time intervals from the specific specified camera or cameras. That is, export up to the time/date and export after the time/date. This may result in multi-time period backups.

The Smart Client – Player can then be used to view the data.

It's recommended that the Data Controller seek legal counsel, conduct both a business impact assessment and a Privacy Impact Assessment (see Conducting an impact assessment on page 28) before the right to be forgotten of the Data Subject is executed, since deletion may introduce new business risks that may tip the balance of interest and introduce risks affecting the privacy protection of other Data Subjects negatively.

Additional safeguards

To better ensure that the Milestone XProtect VMS configuration is GDPR compliant, this list provides you with some additional safeguards to keep in mind when configuring the system.

Issue	Negative impact on privacy	Hints for the controller
PTZ cameras and privacy masking do not work together. The maskings do not follow the PTZ motions.	The privacy enhancing effect of the masking can be circumvented.	Milestone recommends that you do one of the following: • You should not use the XProtect built-in privacy masking feature on PTZ cameras because the mask is static relative to the image's decoded pixels and not the actual direction / location of the PTZ camera. • Deactivate PTZ functionality when you use masks. • Purchase PTZ cameras that support dynamic privacy masking (so the selected areas always are masked no matter the location and zoom of the camera).
Use of microphone or metadata devices may impinge on personal privacy. (In XProtect Corporate, these are by default deactivated.)	The usage of microphones may easily violate GDPR compliance.  Please be aware: Using microphone and metadata devices is not covered by the European Privacy Seal. Their activation would violate the EuroPriSe seal.	Before you activate microphones or metadata devices, you must ensure that you have a clearly justified purpose for collecting data. See Do you have a lawful basis for collecting data? on page 24

Issue	Negative impact on privacy	Hints for the controller
Operators and administrators can export or copy video data, video archives, configuration back-ups and audit logs to local hard drives or removable media like CDs, DVDs, USB flash drives, etc.	Personal data leaves the governance borders of XProtect VMS. The data is not protected by XProtect VMS's access control mechanisms anymore and it cannot be deleted by XProtect VMS when the retention period is reached. This bears the risk that the data is stored longer than allowed, that it is used for different purposes and that the confidentiality of the data is violated.	Data controllers shall take technical and organizational measures to protect data that leaves the boundary of XProtect VMS. See Handling exported data on page 17 for possible measures to take.
Audit log data and other personal data are not encrypted by the product before it is stored in the SQL databases. Database administrators can access audit log data using database clients. XProtect Corporate cannot control or log this access.	Especially, the sensitive audit log data may be disclosed to unauthorised users. See Protecting stored and transmitted data on page 39 and the *Milestone Hardening Guide*.	Do the following: • Implement an adequate role concept for the database administration. • Limit the access to the database to authorized personnel only. • If possible, activate encryption of the database using database mechanisms.
The product implements a back-up feature. This feature backs up the configuration of the VMS but not the audit log database.	A physical destruction of the data carrier that holds the audit log database might prevent the data controller from fulfilling its accountability duties when no back-ups of the audit logs exist.	Consider creating audit log database back-ups. If the Data Controller decides to create backups of the audit log database, one should also establish a process to delete the backups when the retention period is reached and protect it against unauthorised access (for example, encrypting the backup, locking away the backup media, etc.). See the *Milestone Administrator Manual* for more information.

Issue	Negative impact on privacy	Hints for the controller
XProtect VMS uses for some client-to-server and for some server-to-server communication cryptographically unsecured authentication / authorization tokens over unsecured communication channels.	Attackers with access to the network could eavesdrop the tokens and use it to either impersonate VMS users or server components. This could compromise the confidentiality of video data or it could compromise the integrity of the whole system. Please be aware: VPN and / or HTTPS must be configured to protect insecure communications in order to be compliant with the EuroPriSe seal.	Do the following: • Use cryptographically secure VPNs (see the *Milestone Hardening Guide*) • Separate networks (see the *Milestone Hardening Guide*) • Configure https for the Recording Server (see the *Milestone Hardening Guide* and the *Milestone Certificates Guide*.)
The product allows for setting retention times for audit logs, video data, alarms and other personal data.	Setting the retention time to periods that are too long might violate the GDPR requirements for storage limitations (GDPR Article 5 (1) (e) and Article 17).	The retention times must be adapted to the processing purposes (see Right to be forgotten (Right to erasure) on page 31).
Administrators can configure email recipients that may receive video snippets or image stills from the VMS when certain events occur. It is not possible to configure a whitelist of allowed domains for such email recipients.	A typo might possibly lead to a data breach when a third-person receives emails with video data and system alarms.	Make the Data Controller aware of this risk. Milestone recommends that you establish an organizational process such as a four-eyes principle that reduces the risk for failures when entering email addresses.

Issue	Negative impact on privacy	Hints for the controller
Notifications are emails that are sent to a specified email address. When creating a notification, the administrator can choose to include a set of snapshots or an AVI of a sequence.	Because the attached snapshots and AVI sequences in notifications leave the VMS, they are outside the control of the VMS for user access and retention.	Since emails and their content leaves the user access and retention control of the VMS, it is recommended not to attach images or AVI sequences to email notifications. If the customer needs this feature, they at least must ensure that there are organizational procedures and controls for who receives the emails and how they are handled. See Handling exported data in notifications and email on page 18.

Appendix: Data processing in the Milestone XProtect VMS environment

The *Milestone System Architecture Document* describes the components of the system and the way how they interact with each other and with system components of the environment. For each of the relevant use cases of the product you find a diagram that illustrates the communication flow between the components that are involved in the use cases. These diagrams give a general overview about the transferred data.

This section lists the default XProtect installation processes of personal data, authentication and configuration data that are relevant for privacy and security settings.

Personal Data from the VMS

The main data type is the video data from video cameras. This data is stored in the Recording Server. Video data can be either streamed live or in playback modus to the XProtect Smart Client. The other piece of data is the master data of VMS users which is stored in the SQL database.

Personal Data from the Environment

Personal data about the VMS users comes from the Windows environment where Active Direct (AD) is used for user authentication and as a source for group memberships. The XProtect Management Server queries the AD through the LDAP protocol to get information about the user who is logging on to the system.

Personal Data from the System

This personal data encompasses all kinds of data that is needed to secure, configure, operate, maintain or otherwise support the system. Types of personal data include:

- Log data

  IT systems usually log user and system data into audit and debug logs in order to help operate and maintain the systems. XProtect Corporate does so, as well. The VMS logs information about most user actions into the SQL database. This audit log is used to comprehend the accountability for past actions and system behavior and to track misuse of the system. Debug logs are used to identify defects and flaws in the system. Debug data may or may not contain personal data.

  Log and debug data may reveal detailed information about the operators and administrator's usage of the system and may be suitable to monitor employee behavior and performance.

Authentication and Authorization Data

- User Authentication at the VMS

  There are two options to authenticate VMS users at the XProtect Management Client and XProtect Smart Client. You can either use the Windows logon mechanisms or the VMS native authentication.

  In an Windows Active Directory environment, one can configure to use the built-in Windows logon mechanism. Authentication with Windows logon is based by default on the Kerberos protocol. This is the most secure option. In legacy environments domain controllers might not support Kerberos. In this case Windows logon automatically falls back to the NT Lan Manager protocol (NTLMv2), which is deemed to be less secure than Kerberos.

  In environments without a Windows domain controller, you can use the XProtect native authentication method, which is basic authentication with user ID and password against the SQL Server or the Windows for workgroups authentication, if this is available.

  Please be aware: Using the basic user type is not covered by the European Privacy Seal.
  A VMS configuration with basic user type is not entitled to use the EuroPriSe certified product profile. A controller / processor doing so cannot point out that he or she is using a product which especially facilitates data protection and GDPR compliance.

  We thus identify three types of authentication credentials:

  - Windows logon tokens (either Kerberos or NTLM tokens)
  - Basic Authentication credentials
  - Windows for workgroups authentication

After successful authentication, the user is logged on at the VMS and a user session is created at the Management Server, where the logon happens. The client can now access Management Server functionality in the context of this user session. When the user wants to access functionality at the Recording Server, the XProtect Smart Client needs a user session with this server as well.

- User Authentication at the Recording Server

  Since the user session between the XProtect Smart Client / XProtect Management Client and the Management Server cannot be reused to access the Recording Server, the Recording Server needs to authenticate the user as well. In order to authenticate at the Recording Server, the Management Server provides the client with an authentication token, which the client needs to present at the Recording Server. At the same time, the Management Server sends the authentication token to all Recording Servers in the VMS installation. These in turn can be used to authenticate users afterwards.

  XProtect VMS uses a simple GUID as such an authentication token, which the client sends to the Recording Server. The GUIDs are created and managed by the Management Server, which renews these tokens after a specified time period. The GUID is simply an identifier for the user in the SQL Server.

  Please be aware: These tokens are not transmitted in a cryptographically secure way by the VMS and this demands additional safeguards at the network layer of the environment. See Additional safeguards on page 51 for details and Appendix: The Milestone XProtect VMS system and GDPR on page 48 for information about secure networks.
  It is important that you take these an additional steps to ensure that you have a EuroPriSe compliant product.

- Authorization Data

  The authorization data for VMS users is stored in the SQL Server. At the start up time, the Management Server and Recording Server pull the relevant authorization data, including authentication tokens for all users from the SQL Server in order to be prepared for subsequent user access to the servers. When an administrator changes permissions or roles or anything else that effects user authorization, this update is stored by the Management Server in the SQL database on the SQL Server and also actively propagated to all Recording Servers. The Recording Server stores user authorization data and all authentication tokens locally and thus can immediately authenticate XProtect Smart Client users presenting their authentication token.

- Configuration Data

  Apart from view data, which is set by the XProtect Smart Client, all configuration data for the VMS system is configured through the XProtect Management Client of the VMS and stored in the SQL database. There are different types of configuration data:

  - User settings and preferences
  - User permissions
  - Server configuration
  - System settings
  - Camera and device configuration

  While configuration data may not contain personal data, it may affect the way how the VMS processes personal data. For evaluation only, the authorization information and security and privacy settings among the configuration data listed above are relevant.

helpfeedback@milestone.dk

About Milestone

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 Systems 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 Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.