|  |
| --- |
|  |
|  |
|  |
| GDPR Privacy Guide for VMS Operators |
|  |
|  |
|  |
|  |

# As a VMS Operator you must be aware of people’s rights

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.

As a VMS Operator, you have the responsibility:

* Respect people’s privacy. What you see on the screen is confidential.
* Do not use your mobile phone’s camera for recording video of incidents.   
  Instead, use the video push functionality in the XProtect Mobile Client.
* If using video push, filming must be open (no secret video recording).  
  The person who is filmed has the right to know who the VMS controller is and know that the videos can be logged.
* Do not allow non-authorized third parties to view/access the surveillance recordings.
* Do not talk about what you have seen at work with outsiders. Keep it confidential.
* Do not share your account or password, and always log off from the computer at the end of your shift.
* Handle surveillance exports carefully.  
  Exporting is only allowed in coordination with the data protection officer.
* With evidence lock, do not keep recordings indefinitely.  
  You must only keep recordings locked as long as there is a valid reason to keep the recordings, for example an ongoing investigation.
* Notify the VMS controller/your employer without undue delay and implement access control measures in the event of lost equipment such as a mobile device or smartphone.

Remember, there are strict disciplinary consequences as well as criminal and civil law actions if you violate GDPR regulations.

Be aware, too, that your personal data as a VMS operator is subject to data processing. For example, your interactions with the VMS are recorded in the audit log, and if you use a mobile device or smartphone, your usage data may be processed by the vendor of the mobile operating system, unless the capability is turned off. Further, media galleries on your mobile device should not be configured to be backed up to Google or Apple servers. Likewise, if push notification is enabled on your smartphone, data from the smartphone will be processed by the vendor of the mobile operating system.

A close up of a sign

Description automatically generatedWe recommend that you take the short [certification course](https://learn.milestonesys.com/privacy) to improve your knowledge of GDPR.

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