

Information On Data Protection For Video Security Systems (VSS)

Whitepaper



1 Fundamentals Of European Data Protection Law: (GDPR, “Opening Clauses,” FDPA, German Federal Laws)

EU data protection law was restructured with the introduction of the General Data Protection Regulation (Regulation (EU) 2016/679), which came into effect for all member states of the EU on 25 May 2018. As this is a regulation – and not a guideline as had previously been the case – it is legally effective in all countries within the EU. Member states may only enact explanatory or specifying laws in the shape of “opening clauses” as they are known in Germany. If contradictory regulations are thus put in place, the GDPR will take precedence as the superordinate regulation.

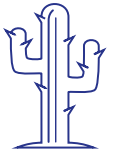
In Germany, the German Federal Data Protection Act (FDPA), which was revised at the same time as the GDPR, features these so-called “opening clauses.” The issue of “Videos” was specified in detail in Section 4 of this regulation. Different specifying laws also apply to Germany’s federal states.

On a European level, Directive 2016/680 was enacted for law enforcement authorities, while Directive 2016/681 was put in place for airline passenger data. These require associated laws to be adopted on a national level in order to be considered legally effective. In Germany, this is implemented through the police laws specific to each federal state, for example.

The Video Surveillance Improvement Law was enacted in Germany in 2016 against the backdrop of the attacks that were carried out in Ansbach and Munich that summer. This was intended to simplify the use of video security systems at large-scale events by outweighing the data subject’s interests in favor of the public authority’s legitimate interest in risk minimization. Significant parts of this were incorporated Section 4(1) of the 2018 revision of the BDGS.

2 Data Protection And MOBOTIX Cameras

MOBOTIX stands for developing and marketing video security systems in the IT sector that satisfy high security requirements. It created the groundbreaking “cactus concept” for IT security to this end.



Its two areas – IoT cameras and MOBOTIX MOVE cameras – pursue the same security objectives, while taking different approaches.

2.1 MOBOTIX IoT Cameras

These cameras stand out due to their decentralized concept, in which image processing, analysis, and storage are carried out on the camera, or are encrypted and controlled by the camera. This offers enhanced system-dependent protection against data loss or third-party access during image transfer.

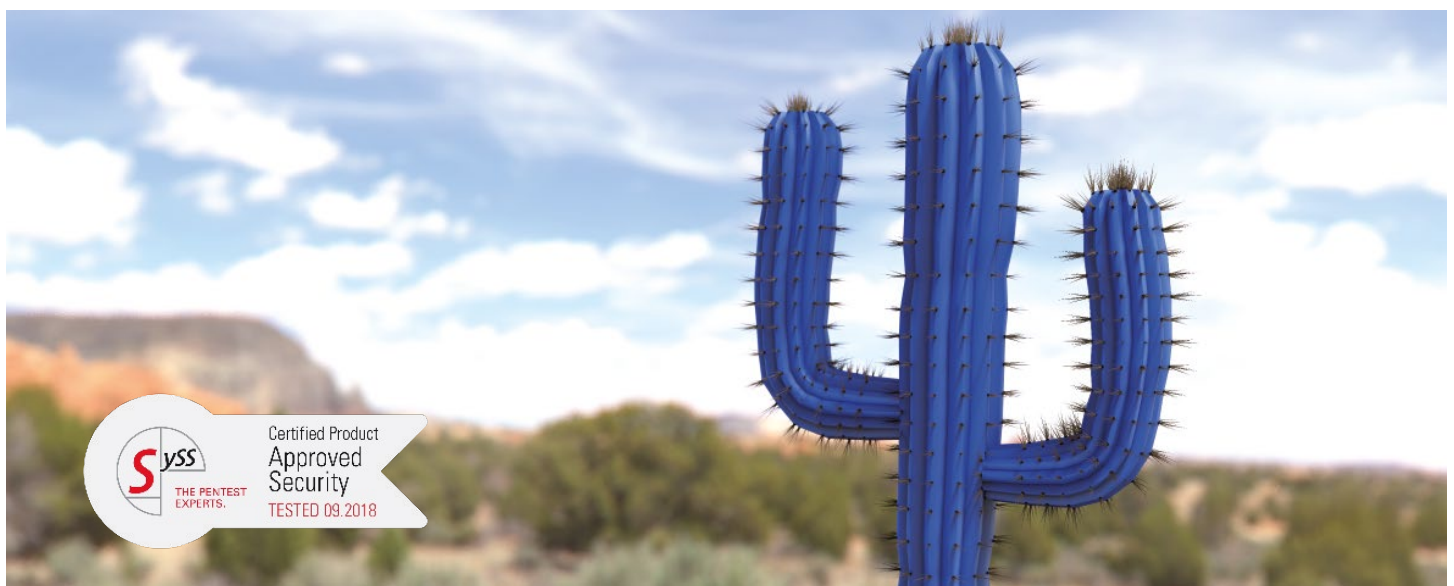
2.1.1 Browser operation

The softbuttons and drop-down menus can be hidden if necessary to prevent unauthorized switching when operating the IoT camera via a browser.

If the “privacy zone” mode is activated in the live view via a softbutton, then access to live images and image searches will be blocked. This setting applies for 24 hours or until it is turned off manually.

2.1.2 Admin area

Different camera security settings can be configured and managed via the Admin area:



a) User rights:

The factory settings allow access to camera images without a password for configuration purposes under the “public access” setting. This access option should be deactivated during camera configuration after changing the admin password or setting up individual users so that accessing the camera is only possible using a password.

The camera is secured by a three-tier rights management system:

Guest: These user rights only allow access to live images with a reduced refresh rate.

User: The setup menu features for image settings, events, actions, and image storage can also be implemented as unlocked browser features on this user level.

Admin: Users on this rights level can configure all security-related camera settings via the admin menu.



b) Admin password:

The first time that a user accesses the admin page they will be asked to change the factory default password “meinsm” to a special password. This must be made up of at least eight characters. Uppercase and lowercase letters have to be observed. Changes cannot be permanently saved in the admin menu if the standard admin password is not changed.

If you forget the admin password, you will need to disassemble the camera concerned and send it to the MOBOTIX headquarters for a hardware reset. In exceptional cases a certified MOBOTIX partner can request a special software with single activation from MOBOTIX to reset the password on site.

c) Microphone:

By default this is switched off on cameras with an integrated microphone. Applying the legal requirement of “privacy by default” guarantees that audio recordings are not made in areas in which this is not permitted by data protection law if the microphone has not been activated manually.

d) Network settings/integration protocols:

This is where not only inputs and profiles needed for integration in networks and third-party systems are administered, but also where different profiles for images, e-mails, and notifications, along with any applicable certificates and access data to third-party systems, are stored and managed. This is generally carried out in the admin area in order to optimally guarantee the data protection principle of access protection.

e) Storage failure detection:

Tests that review the availability, the success of data transfers to a defined storage destination, and successful event playback in the background can be configured via this item in the admin menu. These tests constitute technical and organizational measures (TOMs) on the camera within the meaning of the GDPR. The results of these tests are documented in a logfile on the camera. Should inconsistencies arise, the relevant camera can automatically trigger different types of notifications. These can take the form of flashing LEDs, audio messages, FTP image transfers, error messages in e-mails with/without images, network messages, or even phone calls.

2.1.3 Setup-Area

a) Obscure image areas:

When video security systems are used, it is often necessary for specific areas to not be recorded in general, or to be temporarily hidden for data protection reasons. To this end, image areas to be pixelated as tiles or concealed with colored blocks can be defined in the camera’s setup area. This process is implemented directly on the camera before the images are finalized, and overwrites already existing image information. This makes pixilation irreversible.

b) Arming:

Event control and analytics control are deactivated on all cameras by default according to the principle of “data protection by design and by default” (Art. 25 of the GDPR). To use these features, independent arming can be implemented for storage, actions, and/or notifications after general arming. This makes individual adaptations to a wide range of different data protection requirements possible.

c) MxAnalytics:

Counting corridors and heat maps for statistical purposes can be defined in this area.

1) Counting corridors: “Counting corridors” can be used to obtain information about the number of objects that move through the counting corridors in two different directions. Moving objects are masked as they are detected.

This ensures that faces are not recognizable in the live image, for example. Only the number of objects and times at which they are detected in the counting corridor are saved. No images are stored.

2) Heatmaps:

Movements detected on heat maps are highlighted with colored tiles on the relevant locations. The more tiles that are in the same area, the lighter the relevant color will be (on a scale from dark blue to white). The tiles are saved on a pre-saved reference image during evaluation. Further images are not saved.

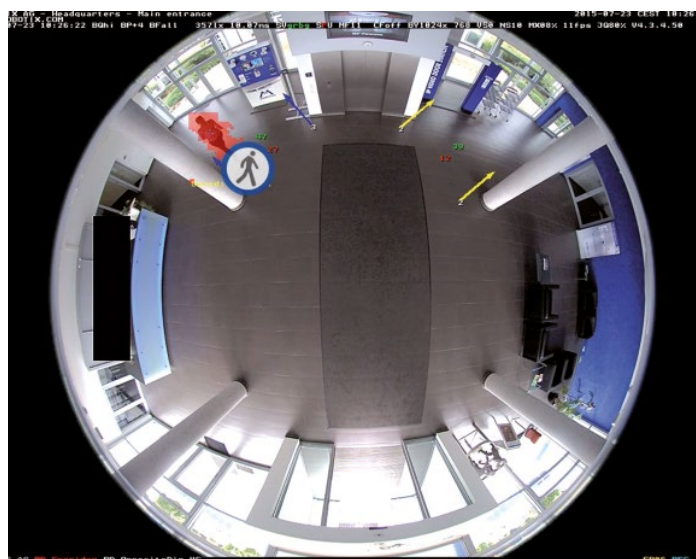
The count statistics and heat map are stored on an SD card separate from the event image storage on the camera, and encrypted using an additional password if necessary.

3) Behavioral detection:

If a camera is mounted to the ceiling, event sensors based on behavioral analyses can be activated alongside counting corridors and heat maps. This measures the following behaviors and values:

- Maximum lingering time
- Movement in the opposite direction to a defined main direction
- U-turn
- Turning from the main direction of movement
- Exceedance of a defined speed
- Entry to a restricted area.

The applicable symbol for the triggering event is displayed on the live or stored images if one of these events occurs. The events triggered by behavioral detection can be used as triggers for a range of different actions, such as saving images, notifications, or switching on warning lights and acoustic signals.



2.2 MOBOTIX MOVE Cameras

a) Admin password::

Just like for IoT cameras, it is also necessary to change the default password “meinsm” to a special password for MOVE cameras when you first log in to ensure legally compliant access protection.

b) Private zones:

A feature for concealing image areas with colored blocks is also directly integrated on MOBOTIX MOVE cameras. This makes it possible to conceal areas that may not be recorded for data protection reasons (for example, during specific time periods). Please note when activating these private zones that the PTZ features are deactivated, as otherwise, the private zone would also be panned during panning of the displayed image area and the wrong image area would be masked.

3 Data Protection And MOBOTIX Software

Information on data protection is included in every piece of software provided by MOBOTIX AG. Different features for ensuring GDPR-compliant video security solutions are also integrated.

3.1 MxManagementCenter

a) Internet connection:

MxManagementCenter can be operated in full without an Internet connection. An Internet connection is only required on two occasions in particular:

1) Software Update:

You have the option of activating a feature under MxManagementCenter’s “Software Update” settings that calls up the MOBOTIX homepage during program launch or at defined intervals to check whether a new software version is available. This feature is deactivated in the factory settings for data protection reasons. This search can also be triggered manually via this menu.

2) Using licensed components:

If MxManagementCenter has to be used with licensed components, an Internet connection will be needed to activate the license code so that the license code’s validity can be verified by the licensing server in the U.S. As MOBOTIX license keys are permanently valid after activation, an Internet connection is no longer needed after activation has been carried out.

b) User management:

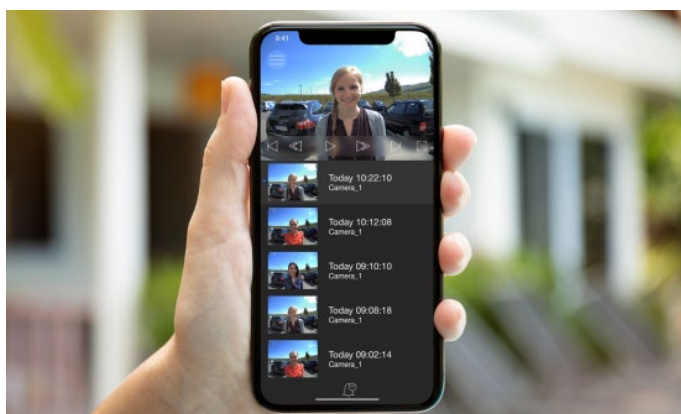
MxManagementCenter accesses assigned video sources (cameras, NAS, etc.) on the admin level in order to control every possible feature of the connected devices. MxMC has a differentiated user management system in order to uphold any differing data protection requirements.

This relates, for example, to the option for restricting access only to defined cameras or activity-related use of features.

3.2 MxBell Doorstation and Camera App

No personal data is collected or stored in the iOS and Android app MxBell on mobile devices (smartphone, tablet).

When granting user rights for cameras, you must check whether the user concerned should receive search rights, for example. These rights also apply to accessing the camera via the MxBell App.



3.3 Older MOBOTIX Doorstation App

The MOBOTIX App can be secured on iOS devices using a PIN code so that only authorized individuals gain access to the MxApp. You can also define which areas/features of the app may only be used by entering this PIN code. This is very helpful, for example, if a user should be allowed to access live images from a door intercom for their job, but should not be entitled to receive access to search stored images via the App for data protection reasons.

3.4 MOBOTIX Partner Tool Box

The MOBOTIX Partner Tool Box is an app for iOS and Android end devices that gives MOBOTIX partners access to documents made available by MOBOTIX in a compact and thematically structured manner. Access to this information is protected by a username and password. Further personal data is not stored.

4 Data Protection On The MOBOTIX Homepage

a) Documents available for download:

MOBOTIX has made a comprehensive range of documents available for download free of charge on its homepage. Along with in-depth technical data and configuration guides, these also include documents on different aspects of data protection.

These documents are available via the link <Disclaimer & Data Protection> in the lower section of each Internet page, or directly via <https://www.mobotix.com/en/disclaimer-and-data-protection>.

b) We also observe the requirements of data protection in a multifaceted way when communicating with our customers. For example, if a customer would like to register for our newsletter on our homepage, they will be notified about data protection regulations and their statutory right of revocation, and have to verify their information and consent. Following the data protection principle of data minimization, every customer also has the option to define topics for their requested newsletter (and to change them at any time) so that they do not receive newsletters that they do not want.

MOBOTIX has developed and manufactured IP video systems, video management and analysis software in Germany since 2000.


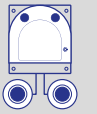


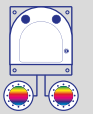
MOBOTIX stands out for its **high level of reliability**. All outdoor cameras are subjected to a stress test for temperatures between -30°C and +60°C (-22°F and +140°F). Without additional components, without heating or cooling and with no moving parts (for example auto iris), they are virtually maintenance free.



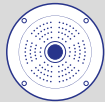

MOBOTIX delivers a **perfectly matched package**, starting with the microSD card for storage management and HD audio (microphone and speaker) with VoIP telephony through video analysis, a professional video management system and motion detection software reducing false alarms.





The **decentralized architecture** means that a central computer is not required and the network load is minimal. The intelligent cameras from MOBOTIX process and store image data themselves, trigger events and, in the event of remote access, manage the frame rate and resolution depending on the available bandwidth.





The **6MP Moonlight sensors** and complementary **thermal imaging technology** ensure reliable detection of moving objects, even under the most challenging light conditions and over long distances. As a result, it is possible to cover large areas with just a few cameras. Less power cabling, less IT infrastructure and fewer additional light sources are needed. MOBOTIX cameras are powered using standard PoE and do not require more than 4-5 watts.


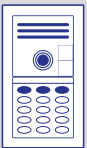


An intelligent IP video system from MOBOTIX allows you to **reduce total costs**. The investment pays for itself after a short time and the free-of-charge software and updates ensure it is a future-proof investment.

Outdoor Dual Lens			Thermal	
M16 AllroundDual	S16 FlexMount	D16 DualDome	M16 Thermal	S16 DualThermal
				
Robust for extreme conditions	Flexible dual camera	Modular dual camera	Thermal dual	Thermal dual

Outdoor Single Lens			
M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Robust for extreme conditions	Discreet, video analysis	Discreet, video analysis	Modular Fix dome

Indoor			
i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° hemispheric	Discreet, video analysis	Modular ceiling camera	Vandalism camera

Door Modules			MxDisplay+
Camera	BellRFID	Keypad	Remote Station
			

Door Station – Example Configurations			
Double Frame		Triple Frame	
			

EN_10/19

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com