Data protection information on video security systems (VSS)

Whitepaper

BeyondHumanVision

MOBOTIX

1 Main features of European data protection law (DSGVO, opening clauses, BDSG, state laws)

European data protection law has been newly regulated for all EU member states by the European General Data Protection Regulation (EU GDPR 2016/679), which came into force on 25.05.2018. Since this is a regulation and not a directive as before, it has direct legal effect in all countries of the EU. Member states may only enact explanatory or clarifying laws in the area of the so-called opening clauses. If this should lead to contradictory regulations, the GDPR as a superordinate regulation has primary validity.

In Germany, the Federal Data Protection Act (BDSG), which was revised at the same time, takes up the opening clauses. Here, the topic of video is specified in more detail in §4. In addition, there are various further implementing state laws in Germany.

Directive 2016/680 was adopted at European level for the area of law enforcement authorities and Directive 2016/681 for the area of passenger data. In order to be legally effective, these require the adoption of associated national laws at the national level. This has been done in Germany, for example, through state-specific state police laws.

In the wake of the attacks in Ansbach and Munich in the summer of 2016, the Video Surveillance Improvement Act was passed in Germany in the same year. This was intended to simplify the use of video security systems at major events by shifting the weighting of the protection interests of the persons concerned in favour of the legitimate interest of the public authorities in minimising risk. Significant parts of this were included in the revision of the BDSG in 2018 in §4 (1).

2 Data Protection in MOBOTIX Cameras

MOBOTIX stands for developing and marketing network-based video security systems that meet the highest quality standards. For this purpose, MOBOTIX has developed the trend-setting "Cactus Concept" for IT and cyber security.

The two product areas MOBOTIX IoT cameras and MOBOTIX MOVE cameras pursue the same security goals from different approaches.

2.1 MOBOTIX IoT Cameras

These cameras are characterized by the decentralized concept, in which the image processing, analysis and storage is performed in the camera or encrypted and controlled by the camera. This offers system-related increased protection against data loss or unauthorized access during image transfer.

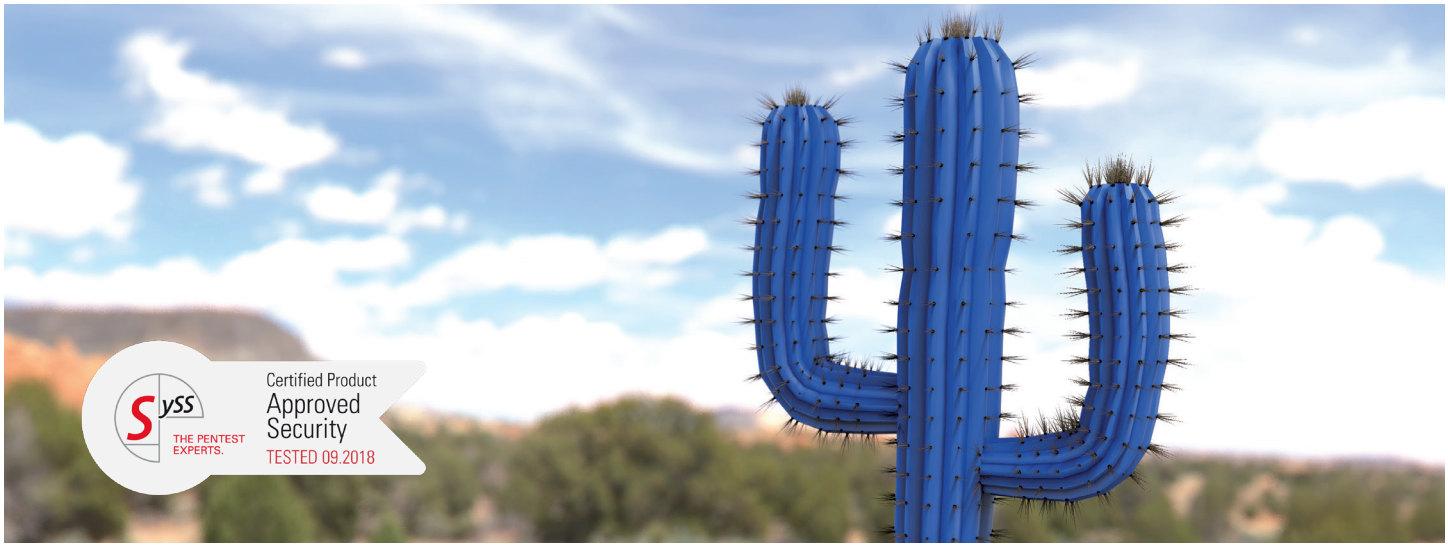
2.1.1 Browser operation

When operating the IoT cameras via a browser, the soft buttons and drop-down menus can be hidden if necessary to prevent unauthorized switching.

If the "Privacy" mode is activated via a soft button in the live view of the browser, access to live images and image searches is blocked. This setting is then valid for 24 hours or until manually cancelled.

2.1.2 Secure connections

The MOBOTIX IoT cameras provide a so-called HSTS function. With HSTS, the browser enforces a flawless HTTPS connection, which provides maximum protection against man-in-the-middle attacks.



MOBOTIX
BeyondHumanVision

2.1.3 Admin Area

The admin area of the camera firmware is used to configure and manage different security settings of the cameras:

a) User rights:

In the factory setting, access to camera images is possible as "public access" without a password for configuration purposes. This access option should be deactivated during camera configuration after changing the admin password or creating individual users, so that all access to the camera is only possible with a password. The camera is protected by a rights management on **three levels**:

- **Guest:** With these user rights, only access to live images with reduced frame rate is possible.
- **User:** At this user level, the setup menu functions for image settings, events, actions, and image storage can be performed as well as unlocked browser functions.
- **Admin:** Users with this privilege level can configure all security-related settings of the camera via the Admin menu.

b) Admin password:

When the admin page is called up for the first time, you will be asked to change the default access data (user: "admin", password: "meinsm") with an individual and secure password. This password must have at least 8 digits. Please pay attention to upper/lower case. Without changing the admin default password, no change can be permanently saved in the admin menu.

If the admin password has been forgotten, it is necessary to disassemble the camera and send it to the MOBOTIX control center for a hardware reset. For a fee, a certified MOBOTIX partner can provide special software individually programmed by MOBOTIX with individual activation for password reset on site (and without camera installation).

c) Microphone:

For cameras with a built-in microphone, this is switched off in the factory setting of the camera firmware. Based on the legal requirements in the area of "Privacy by Default" (security even with factory setting), it is ensured here that no audio recordings are made inadvertently as long as they are not permitted under data protection law. The microphone must always be activated manually first, which is only possible with admin rights.

d) Network settings / integration protocols:

Not only are the entries and profiles required for integration into networks or third-party systems entered here, but different profiles for images, mails, messages and associated certificates and access data to third-party systems are also created and managed. This is generally done in the admin area of the camera firmware in order to optimally guarantee the data protection principle of access protection.

e) Memory failure monitoring:

Via this item, special tests can be configured in the Admin menu of the camera firmware, which check the availability, successful data transfers to a defined storage target and the successful recording of events in the background. These tests represent technical-organizational measures (TOMs) already taken in the camera firmware in terms of the GDPR. The results of these tests are documented in the camera in a log file. In the event of any discrepancies, the camera in question can automatically trigger notifications in various forms. This can take the form of flashing LEDs, audio messages, FTP image transfer, e-mailing of error messages with/without images, network messages or an automatic telephone call by the camera.

2.1.3 Setup area

a) Obscure image areas

When using video security systems, it is often necessary to generally or temporarily hide areas that must not be captured for reasons of data protection. For this purpose, image areas can be defined in the setup area of the cameras, which can be masked either by pixelation as tiles or with full-surface colors. This masking is performed directly in the camera before the images are completed and overwrites the image information available at these locations. This means that the pixelation cannot be undone.

b) Arming:

In accordance with the principle of "data protection-friendly basic settings" (Art. 25 DS-GVO), event control and analytics control are deactivated as factory settings for all cameras. To use these functions, after the general arming, the independent arming of the areas storage, actions and/or notifications is possible. This allows individual adaptations to a wide range of data protection requirements.

c) MxAnalytics Apps:

In this area, count corridors or heat maps can be defined for statistical purposes.

1) Counting corridors:

Counting corridors provide information about the number of objects moving in two directions through the counting corridors. While moving objects are detected, they are masked. This means that no faces are visible in the live image, for example. Only the number and time of the detected objects in the counting corridor and no images are stored.

2) Heatmaps:

In the heatmaps, colored tiles are deposited at the relevant points for detected movements. The more tiles are deposited at the same position, the brighter the respective color (from dark blue to white). The tiles are stored in a pre-stored reference image during an evaluation. No further images are stored. The counting statistics and the heat map are stored in the camera, if necessary encrypted via an additional password, on the SD card separately from the event image memory.

3) Behavior detection:

When a camera is mounted on the ceiling, in addition to the functions of counting corridors or a heat map, event sensors based on behavior analysis can be activated. This involves the measurement of the following aspects:

- Maximum dwell time
- Movement in the opposite direction of a defined main direction
- Reversal of direction
- Turning away from the main direction of movement
- Exceeding a defined speed value
- Entering a restricted area

When one of these measured values is reached, symbols matching the triggering event are displayed in the live or stored images. The events triggered by the behavior detection can be used as triggers for various actions such as image storage, notifications or also switching of warning lights, acoustic signals, etc.

d) MOBOTIX Certified Apps

Starting with the Mobotix7 models, the Certified Apps can be activated in this area. Analogous to the arming, the arming of the app service is also deactivated here as a factory setting for all cameras in accordance with the principle of "data protection-friendly basic settings" (Art. 25 DS-GVO).

2.1.4 End-to-end encryption and deletion periods

a) End-to-end encryption

The basic prerequisite for effective data protection is an activated encryption, because it prevents data from being compromised in the event of theft or loss. To secure stored data, you can enter a keyword under /admin/storageconfig at any time and from the next reboot all new records will be encrypted using this word.

MxFFS encrypts all video content as well as the majority of meta data within each camera using an XTEA-based 128bit process and only transfers this encrypted data to the NAS or file server archive, where it cannot be decrypted by an IT administrator. Decryption is also only performed on the MxMC Client or the playback camera and thus represents an integrated end2end encryption solution.

b) Compliance with the time limits for deletion

After the deletion period has expired, the data is not deleted or overwritten, as in most file systems, but access is made impossible. This is currently "state of the art". (A secure overwrite would halve the lifetime of flash media.)

In addition, the latest software 7.3.0 upwards provides the ability to delete data on the external NAS or file server again by removing all files with video and audio data outside the deletion period.

2.2 MOBOTIX MOVE Cameras

a) Admin password:

As with the IoT cameras, it is also necessary to change the factory admin password "meinsm" to an individual password for the MOVE cameras when dialing in for the first time in order to ensure data protection-compliant "access protection".

b) Private zones:

The MOBOTIX MOVE cameras also have an integrated function for masking image areas with colored areas. This makes it possible to mask areas that may not be recorded, e.g. for data protection reasons (e.g. during certain times). When activating these privacy zones, make sure that the PTZ functions are deactivated, otherwise the privacy zone will be panned along with the displayed image area and mask an incorrect image area.

3 Data Protection in MOBOTIX Software

All software provided by MOBOTIX AG contains information on data protection. In addition, various functions are integrated there to ensure DS-GVO-compliant video security solutions.

3.1 MOBOTIX ManagementCenter (MxMC)

a) Online connection:

MOBOTIX ManagementCenter can be operated completely without an Internet connection. If required, an online connection would only be necessary at two points in time:

1) Software Update:

In the "Software Update" section of the MOBOTIX ManagementCenter settings, you have the option to activate a function that will call up the MOBOTIX homepage at startup or at predefined time intervals to check whether a new software version is available there. This function is deactivated in the factory settings for reasons of data protection. The search can also be triggered manually via this menu.

2) Use of components subject to licensing:

If you want to use a MOBOTIX ManagementCenter with components subject to licensing, you need an online connection or a file that you receive from us to activate the license code in order to check the validity of the license code at the licensing server in the USA. Since license codes at MOBOTIX are permanently valid after activation, an online connection is no longer necessary after activation.

c) User management:

MOBOTIX ManagementCenter accesses the assigned video sources (cameras, NAS, etc.) at admin level in order to control all functions of the connected devices. To ensure different data protection requirements, the MxMC has a differentiated user administration. This includes the possibility of restricting access only to defined cameras or activity-related use of functions. The current version supports the so-called supervisor mode, which supports a maximum of 6-eye control.

The Kaktus concept also applies in the MxMC for the cameras (Secure System in the MxMC components area). It is checked whether all IoT cameras are in the group and whether the default password for the Admin area and the ONVIF area has been changed. It is also checked whether HTTPS is enabled and Public Access is disabled. The MxMC automatically adjusts the settings in the cameras if necessary.

A certificate manager in MxMC allows you to create your own certificates for SSL communication and also manages the distribution of official or your own certificates to the individual IoT cameras.

Every user action in the MxMC that is relevant to data protection is logged in the system's action log.

3.2 MOBOTIX HUB

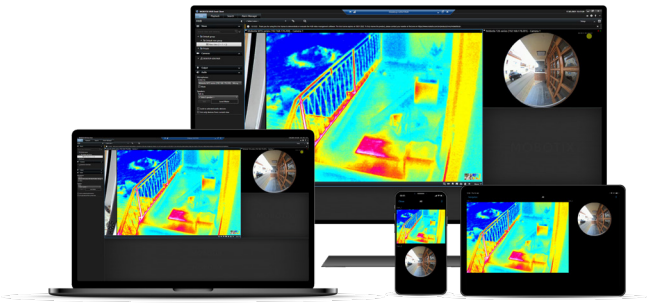
a) Online connection:

Secure encryption and HTTPS connections are provided in the MOBOTIX HUB and we strongly recommend installing SSL certificates for this purpose.

Furthermore, access can also be regulated via individual IP addresses or IP address ranges.

We definitely recommend the MOBOTIX HUB Hardening Guide to configure the system both more securely and in compliance with data protection regulations. You can find it at:

https://www.mobotix.com/sites/default/files/2021-07/Mx_GL_MOBOTIX_HUB_Hardening_V1-00_EN_210701.pdf



b) User management:

A Windows admin account is required to install MOBOTIX HUB. This ensures that no standard users can install or create an admin account on MOBOTIX HUB. For secure user administration, we recommend connecting to the Windows Active Directory.

Passwords for the HUB account must generally be at least 8 characters long, contain upper and lower case letters as well as numbers and special characters.

c) Extended access rights management:

MOBOTIX HUB supports GDPR-compliant access according to the dual control principle. Furthermore, pixelation of camera image areas can be set up so that only authorized users can remove them in the playbacks.

Access to playbacks or live images can be restricted for certain user roles. This can be e.g. the playback duration, as well as the time until when recordings may be accessed in the past.

d) Logs and audit trails:

Accesses are logged so that it can be determined retrospectively which user has changed settings and which, whether he/she has edited alarms or what has been clicked. In this way, manipulations can be easily tracked.

3.3 MOBOTIX Cloud

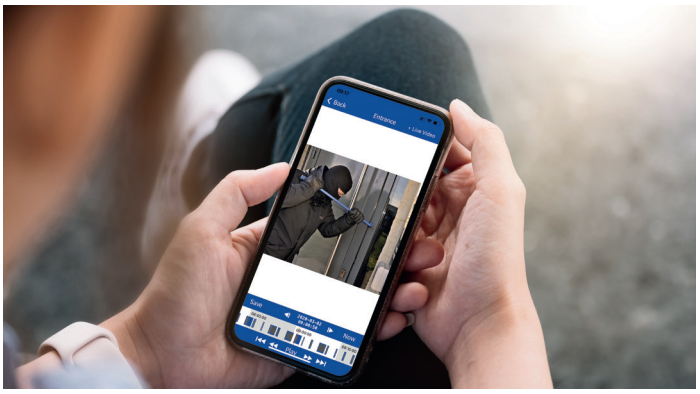
a) Security and data protection:

All communication between cameras, the bridge and the devices is encrypted. Optionally, the 2-factor authentication can be used for more security. Via a fine-granular rights assignment and user administration, you can optimally adapt the rights to your needs and data protection.

All data of our German customers are hosted in data centers in Frankfurt a.M.. The data of our EU customers is hosted on data centers in the EU. The data centers are certified (SOC 1+2, ISO 27001), store the data in triple backups and thus guarantee availability according to DSGVO. A privacy mode is available for end customer subaccounts to restrict (pixelate or hide) image and audio access by the reseller. User activities are stored in the action and audit logs so that changes can be tracked..

b) Bridge

The bridge has no inbound port, so no direct access is possible. Security updates on the bridge are done automatically via the cloud.



3.4 MOBOTIX Live Door Station and Camera App

With the IOS and Android app MOBOTIX Live, no personal data is recorded or stored on the mobile device (smartphone, tablet). When granting user rights on the cameras, it is important to consider whether the user in question should be granted rights for a search, for example. These rights defined in the camera also apply to access to the camera via the MOBOTIX Live app.

The pixelation of the IoT cameras can also be controlled via the MOBOTIX LIVE App. There are predefined API commands that can be activated as softbuttons in the app.

3.5 Older MOBOTIX Door Station App

The use of the MOBOTIX App for IOS devices can be secured with a PIN code so that only authorized persons can access the MxApp. In addition, you can define which areas / functions of the app can only be used by entering this PIN code. This is very helpful, for example, if a user is allowed to access live images of a door intercom for his or her work, but should not be authorised to search through stored images via the app for data protection reasons, for example.

3.6 MOBOTIX PartnerToolbox

The MOBOTIX Partner Toolbox is an app for IOs and Android devices that gives MOBOTIX partners access to documents provided by MOBOTIX in a compact and thematically structured form. Access to this information is protected by user name/password. No further storage of personal data takes place.

4 Data Protection on the MOBOTIX Homepage

a) Documents for download:

MOBOTIX provides extensive documents for free download on its homepage. In addition to a wide range of technical data and configuration aids, this also includes documents on the various aspects of data protection.

The latter documents can be accessed via the link <Liability and Data Protection> in the lower area of each Internet page, or directly via https://www.mobotix.com/en/disclaimer-and-data-protection.

b) We also take data protection concerns into account in a variety of ways when communicating with our customers. If, for example, a customer wishes to register for a newsletter via our homepage, he will be informed of the data protection regulations and his legal right of revocation and must confirm his knowledge or consent by clicking on it. In accordance with the data protection principle of data economy, each customer also has the possibility to define topics for the desired newsletters (and also to change them at any time), so that an unnecessary sending of newsletters is avoided.

EN_12/21

MOBOTIX AG
Kaiserstraße
D-67722 Langmeil
Tel.: +49 6302 9816-0
Fax: +49 6302 9816-190
vertrieb@mobotix.com
www.mobotix.de

MOBOTIX
BeyondHumanVision