

UPDATED  
SECOND EDITION



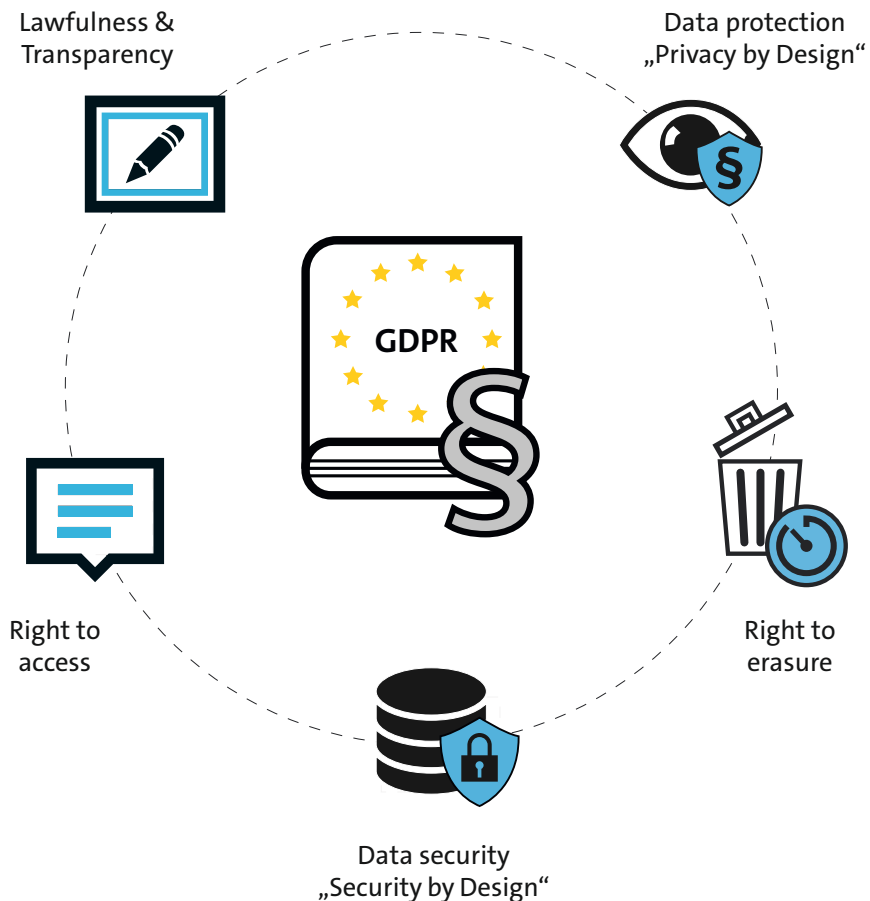
VIDEO SECURITY ACCORDING TO GDPR

# QUICK GUIDE



## COMPANY PHILOSOPHY

# SINGLE SOURCE OF TRUST.

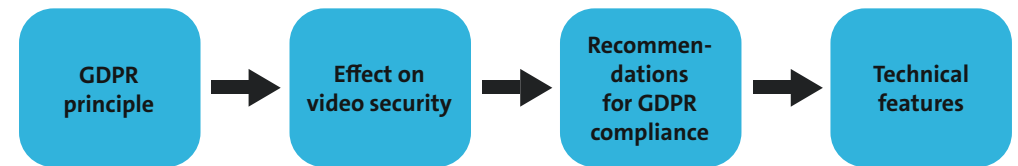


### The „problem“: No specific regulation for video security

The European Data Protection Regulation (GDPR) has been in force since 25 May 2018 in all EU member states, but it does not contain any specific rules on video security. However, where personal data are processed with a video security system, the provisions of the GDPR must also apply to video surveillance.

### The Quick Guide as a helpful guide


This quick guide is intended as a guide for a data controller's video security system (especially for a data controller of a non-public body) to enable GDPR compliance.







Based on five key principles of the GDPR, this quick guide shows the impact on video security systems. In addition, we make recommendations for GDPR compliance and refer to the functions of Dallmeier's data protection and data security module, which can enable GDPR compliance.

### Further information

On page 7 you will find interpretation aids for video security as well as further information on the subject.

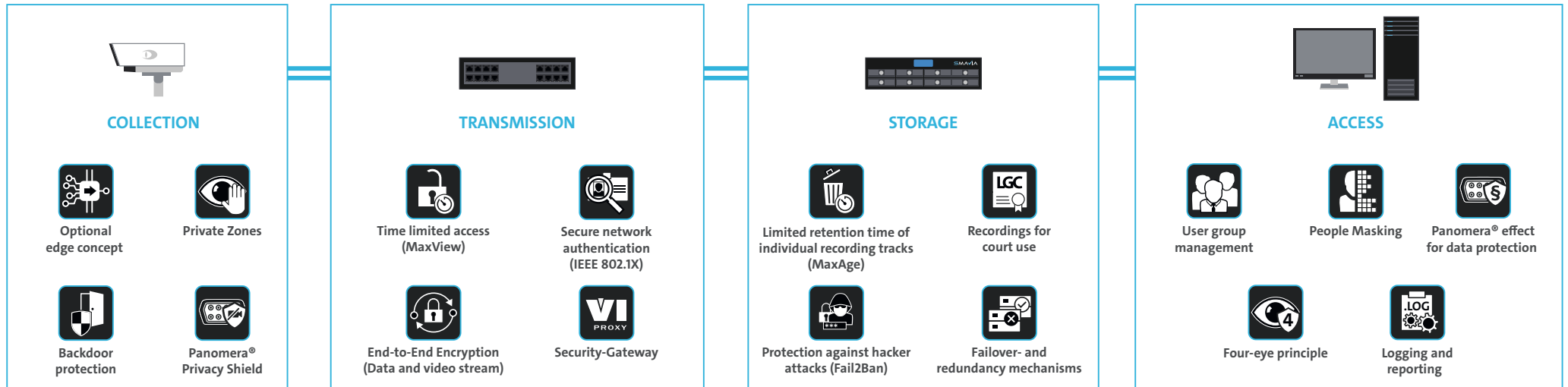
PRINCIPLE	EFFECT ON VIDEO SECURITY	RECOMMENDATIONS FOR GDPR COMPLIANCE	DALLMEIER DATA PROTECTION AND DATA SECURITY MODULE
<b>LAWFULNESS AND TRANSPARENCY OF PROCESSING</b>  	<b>PERMISSIBILITY OF PROCESSING</b> The permissibility of video surveillance is determined on the basis of the following, for example:  Non-public bodies: Art. 6 para. 1 clause 1 lit. f GDPR  Public bodies in certain cases: Art. 6 para. 1 clause 1 lit. e, para. 3 GDPR in relation to a national law  Certain individual cases: Art. 7 GDPR (Consent)	Check and document the legal basis and where applicable the national legal regulations to render the measure of video surveillance purposeful and permissible.  Check the contentual requirements for video surveillance according to Art. 6 para. 1 clause 1 lit. f GDPR in respect of the following criteria: <ul style="list-style-type: none"> <li>• Purposes of legitimate interests pursued by the data controller (e.g. protection from criminal offences, protection of employees / customers)</li> <li>• Necessity (Is the measure suitable for achieving the purpose? Are more moderate measures possible? Is the danger sufficiently real? Have there been incidents in the past?)</li> <li>• Balancing of interests (of the data subject / of the data controller)</li> <li>• Third party interest (Art. 4 No. 10 GDPR)</li> </ul>	Responsibility lies with the data controller of the video security system.
	<b>DATA PROTECTION IMPACT ASSESSMENT</b> In certain cases, which likely result in a high risk to the rights and freedoms of natural persons, a formalized data protection impact assessment (DPIA) must be documented (Art. 35 GDPR).	Check whether a DPIA is necessary. A DPIA shall in particular be required in case of a systematic monitoring of a publicly accessible area on a large scale. (Art. 35 para. 3 lit. c GDPR).  If the DPIA is required, it must be conducted before the measure is implemented and documentation thereof retained.	
	<b>RECORDS OF PROCESSING ACTIVITIES</b> In the records of processing activities (Art. 30 para. 1 GDPR) the video surveillance should be identified and documented, which purpose the processing serves in each case.	Make sure that the video surveillance is identified and documented in the records of processing activities, for which purpose the processing of each individual camera serves in each case.	
	<b>TRANSPARENCY REQUIREMENT AND INFORMATION SIGNAGE</b> Obligations to provide information where personal data is collected from the data subject (Art. 13 para. 1 and para. 2 GDPR).	Make sure that essential information is available for each data subject, e.g. by means of an information sign. Also provide information as to where data subjects can find further, comprehensive information.	Example for an information sign and comprehensive information sheet: See page 7

PRINCIPLE	EFFECT ON VIDEO SECURITY	RECOMMENDATIONS FOR GDPR COMPLIANCE	DALLMEIER DATA PROTECTION AND DATA SECURITY MODULE
<b>DATA PROTECTION</b> <b>„PRIVACY BY DESIGN“</b> 	<b>DATA PROTECTION FRIENDLY SYSTEM DESIGN</b> When purchasing, implementing and operating video surveillance systems the data protection friendly design has to be taken into account.  Appropriate technical and organisational measures are to be implemented to ensure that data protection principles and the rights of the persons affected are safeguarded (Art. 25 GDPR).	Make sure that the video security system is planned and configured carefully and appropriately for its purpose.	<ul style="list-style-type: none"> <li>• <b>Virtual 3D-simulation of projects</b> or davidplan 2D planning tool</li> <li>• <b>Logging and reporting</b></li> <li>• <b>Data minimisation with optional edge concept</b></li> <li>• <b>Panomera® effect supporting effective data protection</b></li> </ul> <p>In addition: See the data protection functions listed below.</p>
	<b>RESTRICTION OF DATA PROCESSING</b> It must be ensured that no personal data outside of the defined and allowed areas is collected.  Check whether pseudonymisation is possible.  Check whether a time restriction on the video surveillance is appropriate.	<p>Make sure that areas of which surveillance is not permitted are blocked out.</p> <p>Make sure that video data that contains personal data is pixelated if this is advisable.</p> <ul style="list-style-type: none"> <li>• If necessary, configure a time-limited recording</li> <li>• Temporarily deactivate the recording completely (recognisable „switched off“), e.g. at peaceful rallies or strikes</li> </ul>	<p><b>Private zones</b>  In addition: Physical alignment of the cameras, alteration of the field of view by zooming, focal length.</p> <p><b>Pixelation</b></p> <p><b>Panomera® Privacy Shield (Privacy „Curtain“)</b>  In addition: Use configuration options for recording times of the Dallmeier cameras</p>
<b>RIGHT TO ERASURE</b> <b>„RIGHT TO BE FORGOTTEN“</b> 	Data from video surveillance have to be erased immediately if they are not necessary anymore for the achievement of the purposes for which they were collected (Art. 17 para. 1 lit. a GDPR) or if the legitimate interests of the data subject are opposed to a further storage.  However, the retention time allowed by the law vary from case to case and must be determined accordingly.	Check the retention time for all cameras and compare them with the documented intended purpose.	<b>Limited retention time of individual recording tracks „MaxAge“</b>

PRINCIPLE	EFFECT ON VIDEO SECURITY	RECOMMENDATIONS FOR GDPR COMPLIANCE	DALLMEIER DATA PROTECTION AND DATA SECURITY MODULE
<b>DATA SECURITY</b> <b>„SECURITY BY DESIGN“</b> 	<b>SECURE SYSTEM DESIGN</b> When purchasing, implementing and operating video surveillance systems the secure design has to be taken into account.  Appropriate technical and organisational measures are to be implemented to guarantee that the level of protection is commensurate with the risk (Art. 32 GDPR).	Make sure that the video security system is planned and configured carefully and with integrated data security functions.	See the data security functions listed below.
	<b>CONFIDENTIALITY (ART. 32 PARA. 1 LIT. B GDPR)</b> Companies should implement security functions which ensure that data of the video security system is kept confidential and protected from becoming known to unauthorised parties.	Check the roles and responsibilities of operators, system administrators and other persons who have access to the system.	<ul style="list-style-type: none"> <li>• User group management</li> <li>• Four-eye-login-principle</li> <li>• Time limited access „MaxView“</li> </ul>
	<b>INTEGRITY (ART. 32 PARA. 1 LIT. B GDPR)</b> Companies should implement security functions which ensure that the data and functions of the video security system are not manipulated inadvertently or deliberately, and consequently that they are genuine, attributable and complete.	Make sure that the data from the video security system cannot be manipulated by impermissible interference.	<ul style="list-style-type: none"> <li>• End-to-end encryption (data and video stream)</li> <li>• „ViProxy“ security gateway</li> <li>• Backdoor protection</li> <li>• Recordings for court use (LGC certificate)</li> </ul>
	<b>AVAILABILITY (ART. 32 PARA. 1 LIT. B GDPR)</b> Companies should implement security functions which ensure that the data and functions are available and are protected from access by external parties.	Take appropriate measures to guarantee that data and functions are permanently available.	<ul style="list-style-type: none"> <li>• Secure network authentication (IEEE 802.1X)</li> <li>• Protection against hacker attacks (Fail2Ban)</li> </ul>
	<b>RESILIENCE (ART. 32 PARA. 1 LIT. B GDPR)</b> Companies should implement security functions which guarantee stability with regard to failures or attacks - e.g. „Denial of Service“ attacks. However, separation from availability is not unequivocal.	See Availability.	See Availability.
	<b>RESTORATION (ART. 32 PARA. 1 LIT. C GDPR)</b> In the event of a physical or technical incident, the availability of personal data and access thereto should be restored quickly.	Make sure that failover mechanisms and redundant components are used.	Failover and redundancy mechanisms
<b>RIGHT TO ACCESS</b> 	The data subjects shall have the right to access to their personal data (Art. 15 GDPR). However, other individuals may also be visible on the video recordings.	Make sure that data subjects who wish to exercise their right to access to their personal data have the ability to exercise this right and can receive a copy of their data. In such cases, other persons must be rendered unrecognisable.	<b>PStream Presenter *</b>  * Function in preparation

## READY FOR VIDEO DATA PROCESSING OF THE FUTURE.

Typical processing of a video security system:



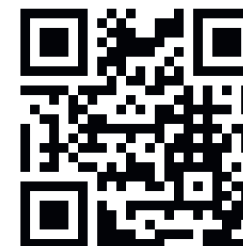
The integrated functions from Dallmeier provide comprehensive protection for a data controller's and / or processor's video security system and help to enable GDPR compliance. Moreover, further data protection and data security functions exist, which you may learn about from the data sheets for the respective Dallmeier products.

**Legal note:** This Quick Guide is intended to serve as a preliminary orientation for a data controller's and / or processor's video security system (especially for a data controller of a non-public body). Please check if further GDPR provisions resp. national regulations pertaining to video surveillance must also be taken into account which apply specifically for example for individual countries / federal states or public and / or non-public bodies.

For example, in Germany the national Bundesdatenschutzgesetz (BDSG) [Federal Data Protection Act (FDPA)] contains a regulation for video surveillance of publicly accessible spaces (§ 4 BDSG) and provisions in the Betriebsverfassungsgesetz [Works Constitution Act] (§ 87 para. 1 No. 6 BetrVG) and the Strafgesetzbuch [Criminal Code] (§ 201, § 201a StGB).

**All information is provided without guarantee and does not replace individual case related data protection advice.**

Visit our web page dedicated to the subject of video security and GDPR. There you will find additional helpful information conveniently in one place:



#### DALLMEIER BROCHURE „VIDEO SECURITY, DATA PROTECTION AND DATA SECURITY“



The brochure provides a detailed explanation of the functions of the Dallmeier data protection and data security module as listed here.

#### MATERIALS OF EDPB



The European Data Protection Board (EDPB) has adopted “Guidelines on processing of personal data through video devices” which contains information on legal requirements and practical examples.

#### TRANSPARENCY REQUIREMENTS AND INFORMATION SIGNAGE

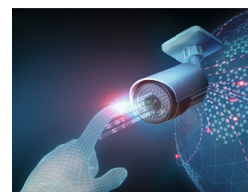


You can also find samples for an information sign and a comprehensive information sheet on the Dallmeier website on video security and GDPR.

#### BE CAUTIOUS WITH GDPR CERTIFICATES

The EU supports voluntary certification programmes and data protection seals for the purpose of increasing transparency and to make it easier to comply with the requirements of the GDPR. However, such certifications only cover processing operations, not products such as a surveillance camera. It is advisable to ensure that certification bodies and data protection certificates have been officially accredited in conformance with the GDPR by a national accreditation body or the supervisory authorities.

#### VIDEO TECHNOLOGY AND CYBERSECURITY



Visit our web page dedicated to the subject of “video technology and cybersecurity”. There you will find helpful best practice information to effectively protect your video security system against cyber threats.





Dallmeier electronic GmbH & Co.KG  
Bahnhofstr. 16  
93047 Regensburg  
Germany

Tel: +49 941 8700-0  
Fax: +49 941 8700-180  
[info@dallmeier.com](mailto:info@dallmeier.com)  
[www.dallmeier.com](http://www.dallmeier.com)