GEUTEBRÜCK

Video Surveillance and the European General Data Protection Regulation (GDPR)

Federal Republic of Germany issue, version: 7/2018

VALUE IMAGING VIDEO SECURITY

Table of Contents

1. General remarks on GDPR

Since 25 May 2018, the European General Data Protection Regulation (GDPR) has finally come into force in Germany after a transitional period of two years. The Regulation contains new rules on the processing of personal data of individuals located within the EU. A revised Federal Data Protection Act (BDSG-new) came into force at the same time as the GDPR.

On one hand, the GDPR establishes principles for the processing of personal data (Art. 5) and the lawfulness of such processing (Art. 6). On the other hand, it formulates obligations for those responsible, data processing companies and data protection officers, gives the parties far-reaching rights to information, regulates the powers of the supervisory authorities (including the imposition of steep fines) and establishes liability claims for aggrieved parties who have suffered material or immaterial damage due to a breach of data protection.

Video surveillance is not explicitly regulated in the GDPR. The new BDSG however contains regulations on video surveillance in public areas in Section 4, which correspond to the previous Section 6b BDSG. Even if the data protection authorities doubt whether the legislator was authorised to do so (there is no corresponding opening clause in the GDPR), these regulations are applicable law in Germany.

Nevertheless, much is still unclear as regards the validity and interpretation of the new regulations, in particular with regard to the operation of video surveillance systems in compliance with data protection regulations. Time will tell how the requirements are to be interpreted accurately.
Therefore, the following information is given subject to correction and can not replace legal advice in individual cases.

2. Design of video surveillance equipment

The operator of a video surveillance system is responsible within the meaning of the GDPR and has to ensure data protection-compliant operation. The installer is not obliged to give any legal advice, but has to inform the operator of the data protection relevance of the collection of images and to support him in the implementation of his data protection obligations. Under Art. 5 (2) GDPR, this can also be seen to apply to the accountability of the operator , which among other things through the creation of a documentation of the technology used.

Insofar as the installer processes (image) data on behalf of the operator himself (for example as part of maintenance or as a service control centre), then he has his own data protection obligations, which are described below.

In the course of planning, the following aspects must be considered by the operator and installer.

2.1 Legality of video surveillance

Any processing of personal data is subject to the principles of Art. 5 of the GDPR, according to which data may only be collected lawfully and for specified, explicit and legitimate purposes (principles of legality and purpose limitation), the collection being for the necessary measure purposes of processing (principle of data minimisation) and processing must be transparent for the data subject (principle of transparency).

For the purpose of a prohibition with reservation of permission,the processing of personal data according to Art. 6, (1) GDPR is only legal if at least one of the following conditions applies:

(a) consent of the data subject
(b) fulfillment of a contract
(c) fulfillment of legal obligations
(d) protection of vital interests
(e) performance of a public task
(f) safeguarding the legitimate interests of the controller

As a rule video surveillance can be justified by applying the last conditions. Consideration must always be given to the personal rights of the data subject. This is also the case for the application of Section 4 BDSG-new, according to which, the monitoring of public spaces is only permitted if it is necessary to safeguard the right to determine who shall be allowed or denied access or for the exercise of legitimate interests for specific purposes and there is no evidence that outweighs the legitimate interests of the data subject.

2.2 Risk analysis - legitimate interests

Before a video security system is designed, the operator must perform an assessment of the threat. He must be able to justify the surveillance and prove that no other means can lead to the same goal at a reasonable cost (keyword: necessity).

Risk analysis includes risks such as threat, fraud, fire, theft, burglary, robbery, sabotage, vandalism, etc., taking into account known incidents, the environment, likelihood of occurrence and potential impact, as well as abstract risks (e.g. at jewellers, gas stations and car parks).

The risks can be used to derive the purposes of the monitoring. Examples include deterrence, education, workplace safety, property protection and access control.

Based on the risk assessment, the components, subsystems and functions of the planned system can be assigned an appropriate level of security from the EN 62676-X-X series of standards. First and foremost this is to determine the required level of data security.

2.3 Operational requirements

The design of the system includes the generation of operational requirements. This is when, among other things, the purpose of the equipment, the required image quality, the recording of images, the operation of the systems and the transfer of data are set.

G Tip:
The BHE offers a checklist for this:
Discussion guide to video analysis.

As a rule, personal data is processed during video surveillance. This is the case if people can be recognised or for example, license plates are legible. This in turn depends on the position, quality and resolution of the cameras as well as the time of use or storage.

2.4 Image quality

The purpose of the system or recording determines the required image quality. In turn the image quality indicates whether the image material is relevant to data protection or not.

The standard EN 62676-4 divides image quality into various categories.

- Low image quality is sufficient for monitoring or detection. Generally, the quality of the images is insufficient to recognise people or to read number plates. In this case, no personal data will be processed, unless a recognisability is possible in conjunction with other data.

- With medium image quality, it is possible to observe or recognise people. Although the image quality is usually not sufficient to recognise people beyond doubt, a match of persons may result from the context in which the images are recorded. Therefore, depending on the context, it would be considered personal data.

- Higher image quality allows the identification or verification of people. In any case, using this image quality, the unequivocal matching to a person is possible and the image processing is clearly relevant to data protection.

- Detailed picture quality criteria and test methods can be found under EN 62676-4 - Video surveillance systems for use in security applications - Part 4 Application rules. The criteria were also adopted under VdS 2366 and the federal uniform directive on alarms and intruder detection (ÜEA, police).

2.5 Data protection impact assessment – Art. 35 GDPR

If a form of processing is likely to entail a high degree of risk to the rights and freedoms of natural persons due to its nature, scope, circumstances or purposes, the person responsible will have a (documented) assessment of the consequences of the intended processing operations. in advance pursuant to Art. 35 GDPR.

According to Art. 35 (3), such a Data Protection Impact Assessment (DPIA) is required, in particular, if a 'systematic monitoring of a publicly accessible area' takes place, which according to the recitals to this provision means monitoring by means of 'optoelectronic devices'.

Where there is extensive and systematic video surveillance of publicly accessible areas (e.g. retail spaces, reception, outdoor areas of a property), a DPIA will always be performed thereafter. This applies more than ever, if analyses take place on the basis of biometric features. According to Art. 9 (1) GDPR, these belong to the categories of personal data that are particularly worth protecting.

Indicators of 'long-range' video surveillance are:

- covering a large area
- moving cameras
- details visible to: recognise, identify and check
- recording > 48 hrs
- employees affected

Tip:
The German Society for Data Protection and Data Security (GDD, Gesellschaft für Datenschutz und Datensicherheit e.V) has published the **GDD practical help guide GDPR X** which provides help to determine if and when a DPIA is to be carried out. See also **Short paper no. 5 on 'Data Protection Impact Assessment'** by the German Data Protection Conference (DSK, Datenschutzkonferenz).
The data protection authorities have recently issued a '**Preliminary list of processing operations**' under Art. 35 (4) of the GDPR, which shows the conditions for conducting a DPIA.

If the data protection impact assessment shows that the processing would entail a high risk for the data subject, the operator must consult the supervisory authorities.
(Art. 36 GDPR)

2.6 Obligation to produce proof

At the request of the data protection authorities, operators must be able to prove that the image data processing complies with data protection requirements (accountability according to Art. 5 (2) GDPR). In terms of video surveillance, meaningful project documentation should be created. The following division of labour is recommended:

Operator:

- Site plan - monitored areas
- Operational requirements
- Inspection plan
- Data protection management system

Installer:

- Design of the systems
- Installation of the cameras used (types and resolution)
- Detailed design
- Inspection results, camera plans with viewing areas
- Description of the equipment (VdS certificate) - see BHE for BHE members

Tip:
The BHE offers various templates on the **home page** (only for BHE members).

2.7 Data minimisation

In Art. 5 (1) GDPR describes the data protection principles, which must also be observed during video surveillance. This specifically concerns data minimisation (1c). In terms of video surveillance, only those images that are necessary or contributing to the purpose of the system may be processed.

G Tip:

Geutebrück offers the right features for this:

- Choice of which cameras are recording
- Privacy masking: blackening of image areas in live, stored and export images
- Privacy masking in cameras (live, stored and export)
- Motion privacy: Pixelation of people or faces in live, stored and export images
- Thermal cameras (live and stored images)
- Rotational operation using dome cameras
- Dome cameras automatically return to home position

2.8 Storage limitations

In most cases records are only needed for a limited period, e.g. until it is clear whether there has been a relevant event. Thereafter, the images must be deleted in accordance with Art. 5 (1e) GDPR and Section 4 (5) BDSG-new.

G Geutebrück systems operate so that the existing data is overwritten after a specified period of several days.

Note: A maximum storage period is not legally explicit. Nevertheless, storage times of 48 to 72 hours have been established in practice. Different deadlines are possibly permitted to bridge weekends or public holidays or for other reasons.

Tip:
The Düsseldorf working group has issued an **orientation guide** on video surveillance by non-public authorities. Storage duration is addressed under point 2.3.1.

Records needed as evidence should be stored on separate tamper-resistant media before the original videotape is deleted.

3. Video surveillance in the workplace

As employees can hardly escape video surveillance carried out in the workplace, there are particularly high demands on their legitimacy. Insofar as the employees have not expressly consented to such measures, or a collective agreement exists, the admissibility of such provisions must be comparable to the principles newly set out in the GDPR and the BDSG.

3.1 Consent

If the video surveillance of employees is based on consent, then in accordance with Section 26 (2) BDSG-new, the assessment of voluntary participation must take into account in particular the dependence of the employed persons in the employment relationship as well as the circumstances under which the consent was granted.

Voluntariness may exist when the employed person has a legal or economic advantage or when the employer and employed person pursue equal interests (e.g. in the case of specific threats). Consent generally needs to be in writing, whereby the employer must first inform the employed person in accordance with the provisions of Art. 7 (3) GDPR on the purposes of data processing and its right of withdrawal. Such consent can be revoked at any time, but is only effective for future recordings (see Art. 7 (3) GDPR).

3.2 Permission in terms of data protection laws

If there is no consent, pursuant to Section 26 (1) (1) BDSG-new, data collection is only permissible within the employment relationship if it is necessary for the decision on the grounds of enforcing or terminating an employment relationship. This regulation corresponds almost word for word to the previous Section 32 (1) BDSG, and leaves room for application in individual cases. According to the previous interpretation, video surveillance solutions should be permitted for access control, employee safety and the vital interests of the officer if employees are given adequate opportunities to withdraw and the measure is otherwise relative.

> **Note:** Only by way of exception, is the covert surveillance of an employee allowed if the strict requirements of Section 26 (1) BDSG-new are met. According to this, factual indications to be documented must substantiate the concrete suspicion that the data subject has committed an offense in the employment relationship.

Furthermore, the nature and extent of the surveillance measure should not be disproportionate to the occasion and should not outweigh the legitimate interests of the data subject. This regulation conforms to the settled case-law of the Federal Labour Court, which also allows an employer to covertly collect data in the case of 'legitimate self-defense'.

3.3 Collective agreements

According to Section 26 (6) BDSG-new, the participation rights of the special interest group of employees remain unaffected by the data protection regulations. This means that in addition to data protection, the collective labour law must be observed, according to which the collection of personal data of employees is subject to co-determination. In accordance with Section 87 (1) (6) of the Works Constitution Act, this covers the introduction and use of technical facilities designed to monitor the behaviour or performance of employees.

Note: Co-determination generally takes place through the conclusion of company agreements negotiated by the management with the representatives of the employees and in which the details of the video surveillance are determined. If the parties have made such a company agreement, any video surveillance provisions carried out thereafter are also permitted under data protection law. This follows from Section 26 (4) BDSG-new, which allows the processing of employee personal data (including special categories of personal data) for employment purposes on the basis of collective agreements.

Note: If the company does not have a works council (for example because it is not the required size of business), the employer should inform the employees concerned early enough - i.e. at the start of the planning phase - about the introduction and use of the video surveillance system and make it clear that the monitoring is not used for behavioral and/or performance control purposes. Declarations of employee consent are only to be obtained in exceptional cases, because in the case of revocation of the consent, the employer could come need to justify their actions in case of revocation of consent. The employer should be transparent in disclosing to employees the reasons for monitoring, balance of interests and provisions taken to protect the data collected, and record all of this with reference to the relevant license facts in his register of processing operations (and generally carry out a data protection impact assessment).

Tip:
Further information can be found in the **DSK Short paper no. 14 on employee protection**.

4. Technical and organisational measures

According to Art. 5 (1) and Art's. 25 and 32 GDPR, the operator of the video system must take all necessary technical and organisational measures (so-called TOMs) to prevent access to the data by unauthorised persons. Video data can also be of interest to perpetrators, for example, for researching the persons depicted or for preparing criminal offenses. For this reason, the issue of cyber security in video surveillance is becoming increasingly important.
Of course, the right choice of monitoring systems and cameras used also contributes to data security.

4.1 Data protection by technology design and data protection-friendly default settings in accordance with Art. 25 GDPR (privacy by design, privacy by default)
Video surveillance solutions from Geutebrück support privacy-compliant operation with a multitude of features. The following description is based on the new requirements of Section 64 BDSG on the security of data processing.

Access control:
- Central access rights management
- Workplace-dependent permissions, separated for live and stored images
- Camera level permissions
- Permissions with time horizon
- Four-eyes principle
- Control of movable cameras with priorities according to alarm or user level
- Integration in domain with single sign-on

- Password protected access
- Passwords encrypted with SHA-256
- Encrypted data storage (GBF proprietary format with AES-256)
- Encryption between all system components
- Bitlocker integration in Windows for encrypting drives (also virtual)

Tip:
See the **statement on Geutebrück system security**.

Transmission control:

- Password protected and encrypted export files with generic video format MP4/H264EAW with Geutebrück RSH-1024 signature
- Watermarked export files with M4A signature
- Adjustable storage options for export
- Certified interfaces (SDK) for the connection to G-Core

Tip:
Further information can be found at BHE: **Cyber security in video systems**.

Input control:

- Binding time in the overall system
- Audit trail: tamper-evident protocolling of user-related activities, e.g.
  - Login at the workplace
  - Authorisation attempts without permission
  - Selection and duration of the viewing cameras
  - Viewing stored images
  - Finding images (motion search)
  - Exporting of images and to where
  - Changes of settings, processing of alarms

Availability control:
To ensure the availability of data, Geutebrück provides the following redundant systems:

- Multispare
- Failover
- Edge recording

Wherever possible, the features are factory-designed to ensure the highest level of privacy possible (privacy by design).

- Restriction of administrator permissions
- Clear installation and operating instructions as well as online help

Tip:
For training and webinars regarding optimal adjustment and the handling of Geutebrück solutions, please inquire at the **Geutebrück Academy**.

4.2 Provisions for data protection and data security by the operator and installer

Aside from the security measures integrated in the video solutions, the operator and installer must also take appropriate data security measures to prevent access to data by unauthorised persons (privacy by default).

a) Physical security (access control)

- Access to buildings
- Access to servers
- Access to terminals

b) Organisational provisions

- Training of employees/security officers
- Contracts with service companies for the purpose of order processing according to Art. 28 GDPR (for example for external security service companies)
- Defining procedures for dealing with the data
- Requests from data subjects, procedure for data breaches, password management.

c) Technical provisions during commissioning

- Hardening systems

Tip:
See the Geutebrück **Hardening Guide**.
Geutebrück offers various support services e.g. patch management. Please contact our central support team.

d) Maintenance

It is recommended to keep systems continually up to date. This refers to both the network systems and components such as the solutions by Geutebrück.

Tip:
Geutebrück provides regular information and recommends a timely update of the systems concerned. The respective updates are always tested before release regarding the effect on functionality and performance. Current versions can be found as a registered member of the **WebClub** on the Geutebrück homepage, under Software Downloads.

- Latest releases of G-Core, G-SIM and other products with new features and improvements in security
- New firmware versions for hardware components and cameras
- Latest bios updates of the motherboard manufacturer
- Latest Windows updates with security patches

G Tip:
Geutebrück also offers suitable **maintenance services**.
Please contact our **central support.**

Note: Please note that if you commission service providers or manufacturers such as Geutebrück in the case of support (repairs, maintenance), these companies are considered to be data processing companies in accordance with Art. 28 GDPR and must uphold their obligations.

G Tip:
Geutebrück offers a standard draft contract for this purpose. Please contact your **sales** representative.

5. Transparency and obligations to report

According to Section 4 (2) BDSG-new, appropriate measures should be taken to make the surveillance and the officers name and contact details identifiable as early as possible. This is usually done by signs that may be read by the data subjects before they get into the detection range of the cameras.

5.1 Information obligations

According to the provisions of Art. 13 GDPR, the signs must however also contain further information that has to be communicated to the data subject 'at the time when personal data are obtained'. In order to fulfill these information obligations, the data protection authorities recommend a graded distribution of information.

This means that before entering the area to be monitored, a sign displaying the essential information (so-called 'upstream information sign') must be provided.

- Most importantly, this sign is to contain a pictogram of the camera symbol, the name and contact details of those responsible, the contact details of the data protection officer, the purpose and legal basis of the processing and where applicable, the legitimate interests and the storage period. There should also be a reference to further information.

- A detailed information sheet must be affixed or kept at another, easily accessible place. This can also be on the internet. Here, in addition to the above-mentioned information, the rights of the data subject to information, objection, deletion and complaint in relation to the supervisory authority are documented.

According to Art. 12 (7) of the GDPR, the information must provide a meaningful overview of the intended processing in a way that is easily visible, intelligible and clearly legible.

Tip:
The Niedersachen State Commissioner for Data Protection has issued **examples of an upstream information sign and a complete information sheet**.
The BHE also offers information on **GDPR compliant signage for BHE members**.

5.2 Rights of the persons concerned

With regard to the rights of the data subject, there are some special features to be considered in video surveillance. In addition please see the following notes:

Right to information (Art.15 GDPR)

Note: If the request for information is too vague and the effort becomes too great or the person concerned can not possibly be identified, the operator is not obliged to provide any information. Otherwise, in accordance with Art. 12 (3) GDPR, the information to be provided must be provided promptly, and in any event within one month following receipt of the application.Since the pictures are usually. overwritten after a few days, the request often takes care of itself. If other persons are also visible in the pictures, no copies of them may be passed on if this could impair the personal rights and freedoms of these persons (see Art. 15 (4) GDPR). A corresponding response with explanation of the facts is nevertheless necessary.

Right to rectification (Art. 16 GDPR)

Note: The right of rectification is limited in that the video recordings generally can not be technically changed or may not be changed to preserve the authenticity of the data.

Right to erasure (‘right to be forgotten’) (Art. 17 GDPR)

Note: The right to be forgotten is usually. ensured by automatic overwriting. If no dedicated storage ensues, for example, in the event of an alarm, the images are stored in another ring buffer and therefore available longer for evaluation and proof purposes.

Right to restriction of processing (Art. 18 GDPR)

Note: This right is taken into account due to automated data deletion by overwriting and purposive retention.

Right to data portability (Art. 20 GDPR)

Note: It should be noted here that the transfer is technically possible only to a limited extent. In addition, a transfer may affect the rights of third parties.

Right to object (Art. 21 GDPR)

Note: This right is taken into account due to automated data deletion by overwriting and purposive storage.

Right to lodge a complaint (Art. 77 GDPR)

Note: Complaints can always be addressed to the company data protection officer.
There is also the possibility to complain to the Data Protection Inspectorate.

The operator must establish a regulation, which ensures that the concerns of the data subject are promptly answered in an understandable form, regardless of whether it is technically or legally possible to implement the claims.

6. Other duties, sanctions, processing of data

Further data protection responsibilities should be pointed out with due brevity:

6.1 Further data protection obligations

According to Art. 30 GDPR, all processing of personal data must be included in a list of processing activities. As a rule, this also applies to video surveillance. The documentation includes, amongst other things, the purpose of the processing, legal basis, categories of data subjects, categories of data, recipients, deletion periods and technical and organisational measures.

G Tip:
See also **Short paper no. 1 Records of processing activities - Art. 30 GDPR.**

The operator of a video surveillance system will also have to appoint a data protection officer, which they will need to register with the competent state data protection authorities (Art. 37 GDPR). According to Section 38 (1) BDSG-new, an officer is to be appointed regardless of the number of employees if processing takes place in the company which is subject to a data protection impact assessment, which is often the case with extensive and systematic video surveillance in publicly accessible areas.

It is also the responsibility of the operator to define and document responsibilities and processes to ensure privacy compliant operation. For example, it must be ensured that supervisors are notified within 72 hours in the case of data loss whereby the breach of the protection of that data creates a risk to the rights and freedoms of individuals.

6.2 Sanctions and responsibility

Violation of the aforementioned data protection obligations may be subject to high fines by the competent supervisory authorities (i.e. the state data protection officers). For example, in the absence of a data protection impact assessment or in the absence of a list of procedures, a fine of up to €10 million or, in the case of a business, up to 2% of its total worldwide annual turnover in the previous financial year may be imposed. Infringements of the principles of data processing or the conditions for eligibility under Art. 5 and 6 of the GDPR can even lead to fines of up to €20 million and, in the case of a business, up to 4% of the total worldwide annual turnover.

Furthermore, in the future, the data subject can assert claims for damages against the officer if they have suffered material or immaterial damage as a result of a violation of the GDPR (see Art. 32 GDPR). Collective actions are also possible in the future (see Art. 80 GDPR), so that such claims can also be asserted in bundled form by interest groups.

6.3 Processing of data

Such sanctions and liability risks can not only affect the operator of a video surveillance provision as the originator, but also all service providers who assist the operator in this regard and participate in the processing of the image data collected by the surveillance (so-called "order processor" within the meaning of Art. 28 GDPR), if they violate the data protection obligations arising in this context. This primarily concerns control centres to which monitoring images are applied.

According to the data protection authorities, the regular maintenance and parameterisation of a video system is considered to be order processing if the service provider has the necessity or the mere possibility of access to personal image data.

Tip:
Further prerequisites for order processing can be found in the DSK **Short paper no. 13.**

In such cases, the person responsible must contractually oblige the processor to apply the same data protection care when processing the personal data, which is the responsibility of the officer. Details are regulated under Art. 28 GDPR, which imposes extensive obligations on the parties of such a contractual relationship. In the case of ongoing maintenance contracts, it is likely the parties will also have to conclude a separate contract for order processing in the future. Whether this also applies in the case of one-off planning, construction and commissioning of a monitoring system, which is not further maintained by the installer, is to be examined in the respective individual case.

7. Documents and sources

Geutebrück

- **Statement on Geutebrück system security**
- **Geutebrück Hardening Guide**
- Checklist 1: General requirements of the GDPR for video surveillance systems
- Checklist 2: Requirements for compliance with data protection principles according to the GDPR
- Checklist 3: Requirements regarding data security according to the GDPR
- Checklist 4: Requirements regarding cyber security according to the GDPR

The Society for Data Protection and Data Security

- **GDPR practical help**

Country Commissioner for Data Protection

- **Examples of an upstream sign and a complete information sheet**
- **Provisional list of processing operations under Art. 35 (4) GDPR**

Düsseldorf working group

- **Orientation guide** on Video surveillance by non-public authorities.

Data protection conference

- **Overview of GDPR short papers**
- **Short paper no. 15 - Video Surveillance under the General Data**
- **Protection Regulation**
- **Short paper no. 14 - Employee Data Protection**
- **Short paper no. 13 – Order Processing**
- **Short paper no. 5 - Data Protection Impact Assessment**
- **Short paper No. 1 - Procedure index of processing activities**

BHE

- Checklist - **Discussion guide to video analysis**
- **Important notes for installers - cyber security in video systems**
- **GDPR compliant signage (only for BHE members)**

No responsibility is taken for the content of this white paper. The document does not replace legal advice.

Responsibility for the content of linked documents is borne by the respective author. Please also read the disclaimer on the Geutebrück website.

For a legal consultation,
we recommend the
law firm Dieckert.

Please note that this advice
is chargeable.

DIECKERT
Recht und Steuern
Gertraudenstraße 20
10178 Berlin

Telephone: +49 (0)30 27 87 07
Fax: +49 (0)30 27 87 06
Email: ulrich.dieckert@dieckert.de
Website: www.dieckert.de

Imprint
GEUTEBRÜCK GmbH
Im Nassen 7-9
D-53578 Windhagen
Tel.: +49 (0) 26 45 /137 - 0
Fax + 49 (0) 26 45 /137 - 999

Managing Directors:
Katharina Geutebrück
Christoph Hoffmann
Commercial registry: HRB 14475 Montabaur
Tax identification number: DE813443473
info@geutebrueck.com

VIDEO SECURITY VALUE IMAGING

www.geutebrueck.com

Follow us on

GEUTEBRÜCK

General requirements of GDPR video surveillance systems

This checklist is intended to aid the operator of the video equipment in the awareness of their privacy obligations.

GDPR reference	Item	Comment	Fulfilled
Art. 30	List and description of processing activities		
Art. 37	Appointment of a data protection officer		
	Notification of the data protection officer to the state data protection authorities	See also: bfdi	
Art. 6	Test of legality of video surveillance		
	Works council integration		
Art. 5 (2)	Accountability - Documentation		
	■ Risk analysis		
	■ Operational requirements		
	■ Inspection plan		
	■ Design of the systems		
	■ Installation of the cameras used (types and resolution)	See EN 62676-4	
	■ Detailed design		
	■ Inspection results, camera plans with viewing areas		
	■ Description of equipment (VdS certificate)		
Art. 35	Data protection impact assessment (DPIA)		
Art. 36	The involvement of data protection authorities according to the DPIA		
Art. 13	Transparency and obligations to report		
	■ Information sign in the access area		
Art. 15	■ Further information and rights of the data subject		
Art. 33	Process definition for data loss	Notification of the data protection authorities - Notification of the data subject	
Art. 15	Process definition for requests for information from the data subject	Right of access, correction, deletion	
Art. 28	Contracts on processing of data	Security service companies	

Requirements for compliance with data protection principles according to the GDPR

These are a selection of systems, products, or features that help ensure compliance with data protection requirements.
Depending on the situation, different elements may be required.

GDPR reference	Item	Comment	Fulfilled
Art. 5c)	**Data minimisation**		
	Use and installation of cameras		
	Targeting non-sensitive areas		
	Privacy shield guard	Avoidance of test pressure	
	Moving cameras	Avoidance of test pressure	
	Thermal cameras	Difficulty of identification	
	Rotational operation using dome cameras		
	■ Adjustable rotation	Predefined non-sensitive image areas	
	■ Automatic return to home position		
	Blackening out of image files	**Privacy masking**	
	Live mode	See EN 62676-4	
	Stored images	The blackened out parts can be removed if necessary	
	Exported images		
	In camera settings		
	Pixelation of persons or license plates	**Motion privacy**	
	Live mode		
	Stored images		
	Exported images		
Art. 5 e)	**Storage limitations**		
	Overwriting data	Dependent on storage size	
	■ Normal video images	Typically after 3 to 5 days	
	■ Alarms and events (in separate ring buffers)	Depending on the purpose of storage (e.g. at ATMs)	

Requirements regarding data security according to the GDPR

This is a selection of provisions structured according to Section 64 BDSG, which contribute to data security. Depending on the situation, the correct selection of data security provisions contributes to the desired or required security level.

Section 64 BDSG	Item	Comment	Ful-filled
	Access control	**Physical security**	
	■ Access to buildings		■
	■ Access to servers		■
	■ Access to terminals		■
	Data media control	**Export files and backup files**	
	■ Selection of suitable export media (password-protected)		■
	■ Encryption		■
	■ Password-protected		■
	■ Watermarks in export files		■
	Storage control	**Password protection**	
	■ Password according to BSI specifications		■
	■ 4-eyes principle		■
	■ Integration in domain with single sign-on		■
	■ Password protected remote access		■
	■ Password encrypted		■
	■ Encrypted data exchange between the system components		■
	■ Drives (Bitlocker)		■
	User control	**Watermarked export files**	■
	Access control	**Rights and role concepts**	
	■ Authorisation groups		■
	■ Administrators		■

Section 64 BDSG	Item	Comment	Ful-filled
	Access control	**Group permissions for...**	
	■ Maps		■
	■ Treatment of live/stored/exported images		■
	■ Camera level permissions		■
	■ Temporary access		■
	■ Privacy masking		■
	■ Motion privacy		■
	■ Video analysis		■
	■ Alarm management		■
	Transfer check	**Audit trail**	■
	Incoming control	**Recording** **User-related activities**	
	■ Binding time/date specification		■
	Transport control	**Encrypted export files**	■
	Recoverability	**Contingency plan**	■
	Reliability	**Monitoring and fault clearance**	
	■ Diagnosis tools		■
	Data integrity	**Data protection concept**	■
	Job control	**Data processing according to direction and guidance**	
	■ Contract for commissioned data processing		■
	■ Training security officers		■
	Availability control	**Protection against accidental destruction and loss**	
	■ Multispare redundant systems		■
	■ Failover		■
	■ Edge recording		■
	■ Data protection		■
	■ Antivirus protection		■
	Separability	**Obligatory separation for earmar-king**	
	■ Authorisation scheme		■

Requirements regarding Cyber Security according to GDPR

Currently, protection against access by unauthorised persons presents special challenges. Depending on the required level of protection, sufficient safeguards must be taken against cyberattacks according to the level of the technology.

GDPR reference	Item	Ful-filled
Art. 25	**Network security**	
	■ Separation of CCTV network and other networks	☐
	■ Use of VLAN	☐
	■ Secure external connections via gateways	☐
	■ Restriction to MAC addresses	☐
	■ WLAN avoidance	☐
	■ Use of a firewall	☐
	■ Remote access over VPN	☐
	■ Antivirus software	☐
	Secure connection between all system components	
	■ Encrypted transmission between all components	☐
	■ Fixed IP addresses	☐
	■ Deactivation of SSH access	☐
	■ Deactivation of Multicast	☐
	■ Deactivation of QoS	☐
	■ Change default ports	☐

GDPR reference	Item	Ful-filled
Art. 25	**Passwords and user management**	
	■ Change default password Geutebrück system admin	
	■ Change default password Geutebrück operating system	
	■ Change default password all G-Core clients and services	
	■ Change default password G-Health	
	■ Change default password G-SIM	
	■ Change default password G-Link	
	■ Change default password GeViSoft	
	■ Change default password GeViScope	
	(Password assignment according to BSI specifications)	
	Windows operating system	
	■ NTP time synchronisation	
	■ Deactivation of unused services	
	■ SQL Server access without administrative capabilities	
	■ Maintenance contracts for the regular updating of the systems	