

Data Protection Concept Technical and Organisational Measures within the meaning of Art. 32 para. 1 GDPR (DSGVO)



1 Document Information

The EU General Data Protection Regulation (GDPR) and the new version of the Federal Data Protection Act (BDSG-neu) contain guidelines on how to deal with personal data from a technical and organisational point of view. This serves the purpose of data security. Data security thus represents a further and complementary aspect of data protection.

Data security is regulated by law in Art. 32 para. 1 GDPR. The rules require that such technical and organisational measures be taken as are necessary to ensure the protection of personal data.

The GDPR names various control areas, each of which contains different sub-points:

1. Confidentiality
2. Integrity
3. Availability and resilience
4. Procedures for periodic review, assessment and evaluation
5. Pseudonymisation and encryption

2 Version History

Version	Status	Date	Responsible	Modification
4.0	Release	10.02.2021	DCO	Review and release
4.1	Adaptations and release	20.07.2022	DCO	Amendment / integrity transfer control
4.2	Adaptations / updates	24.07.2023	DPO / IT	Reference to ISO 27001 certification Amendment of Contract Data Control Amendment of Entry Control, Transfer Control and Availability
4.3	Current CI	25.07.2023	DCO	Format adaption
4.4	Adaptation/update		DPO / IT / DCO	Amendment of security measures
4.5	Adaptation/update	22.09.2026	DPO	Review and amendment of current security measures
4.6	Review/update	24.09.2026	IT	Comprehensive review and amendment of current security measures Format adaption
4.7	Review/addition	25.09.2026	DPO	Final review, amendments and approval
5.0	Release	25.09.2026	DPO / DCO	Format adaption

3 Organisational Aspects

KUMAVISION AG has appointed an external Data Protection Officer, in the person of Maximilian Musch - Deutsche Datenschutzkanzlei - in accordance with Art. 37 GDPR and Section 38 para.1 BDSG-neu (Federal Data Protection Act, new.) Those employed in the data processing are bound in writing to maintaining data secrecy as well as confidentiality. The Data Protection Officer and data protection coordinator carry out monitoring audits on a regular basis, as well as subject-specific training.

KUMAVISION AG ensures the written documentation of the current data protection level, as well as the written work instructions, guidelines and data sheets for employees. A data protection area on the intranet as well as general and subject-specific action aids, guidelines, factsheets, awareness training etc. are used to train and raise awareness as well as maintain the level of security. In addition, procedures/processes are implemented in the area of change and risk management, notification, reporting of incidents, requests for information, as well as requests for correction, deletion and blocking (in addition see section 4.4).

4 Security Measures

The following points describe the technical and organisational measures implemented by KUMAVISION AG for data protection in accordance with Art. 32 para. 1 GDPR.

The servers, databases and the backup are operated and maintained at KUMAVISION AG or by commissioned third parties in professional computer centres. (Data centres with documented physical, technical and organisational security measures, as well as appropriate evidence of audits or certification.) The subcontractors are carefully selected and reviewed with respect to their security awareness and expertise.

Some of the security measures in the following checklist relating to this area are not indicated separately, because they lie within the responsibility of the subcontractors, or they are not published in detail for reasons of maintaining security through confidentiality. More detailed information on the data protection/data security processes as well as the review and control of the measures implemented can be found in section 4.4 ("Procedure for regular review, assessment and evaluation").

4.1 Confidentiality (Article 32 para. 1 (b) GDPR)

4.1.1 Entry Control

Entry control includes measures that are appropriate for preventing unauthorised persons from accessing data processing systems.

#	Measures
1	The entry control to KUMAVISION's network rooms is ensured by the spatial structure of the respective building and the control systems used there (restrictive, documented, double access authorisation procedure: card and key; locked doors; intruder alarm system). Entry control to the data centres of the various cloud providers is ensured through a range of measures implemented by the operators. They also hold the relevant certifications for this.
2	An appropriate locking system is used for the required data protection (keys; chip card/transponder locking system; code lock).
3	Visitors: registration via intercom for permission to enter buildings, or for pick-up/receipt/entry by site assistance.
4	A responsible person is delegated for the administration of the means of access.
5	A documentation of the means of access is maintained and continuously updated (register).
6	In the event of loss, means of access will be blocked immediately (blocking of chip cards/transponders).
7	Lockable individual offices in most cases.
8	Buildings or premises are locked and can only be opened manually by the employees.
9	An alarm system secures the building against unauthorised access, including outside of business hours.
10	The archive is also locked and may only be accessed by authorised employees (management, accounting).
11	Visitors are only permitted to remain on the business premises when accompanied by an employee. Maintenance services and visitors to the network rooms are constantly monitored/escorted.
12	Logging of access-control systems to track the entry/exit of specific premises, areas and protected zones. Regular evaluation in the case of any abnormalities, as well as after (potential) security breaches.
13	Return or removal of means of access when employees leave the organisation or relocate.

4.1.2 Data Access Control

Measures suitable for preventing data processing systems from being able to be used by unauthorised persons.

#	Measures
1	Reduction of the persons with authorised access to a minimum.
2	Client systems can only be used after password-based authentication.
3	A mandatory procedure is implemented for assigning authorisation.
4	Unauthorised persons are denied access to the corporate network and to IT services. Login is only possible with a registered user account, password and MFA (multi-factor authentication).
5	The guest WLAN is separated from the company network.
6	A clear assignment of user accounts to users is possible.
7	Use of firewalls and intrusion detection systems for the prevention and detection of attacks.
8	A password policy with a sufficient standard of protection is implemented (12 characters minimum with upper case, lower case, numbers, special characters (3 criteria must be met)). Additional specifications for the structure of the password (e.g. account name or more than two characters from the user's full name may not be used); reporting channels in the case of a third party being suspected of knowing the password; replacing initial/one-time passwords after first use
9	Virus protection programs (client and server) are available and are always kept up to date (all clients and servers). Threat protection is ensured for the entire M365 environment with MS tools.
10	Use of a central spam filter + phishing filter (central incoming email). Emails are flagged and forwarding is prevented, if applicable. Use of automatic updates and signature recognition.
11	To protect email communications, technical measures are used to authenticate senders, detect identity theft and filter out harmful content. The configuration and effectiveness of these measures are monitored on a regular basis.
12	Automatic screen locks when leaving the workstation (password-protected) are controlled by an internal policy. Automatic logout from systems in the case of longer periods of inactivity.
13	Functional restriction of the use of workplaces (restrictive allocation of rights according to function/activity).
14	Centralised patch management and automated distribution of software and operating system updates and patches within the company. Updates/patches cannot be bypassed, and/or they are automated. Only approved patches/updates can be installed.
15	Regular automated vulnerability scans of IT systems. Identified vulnerabilities are assessed, prioritised and rectified within defined timeframes based on their level of risk.
16	Performance of penetration tests to check the security architecture and the measures used.
17	Centralised device management (laptops and smartphones) using an MDM solution
18	Network monitoring with alerting
19	Terminals are hardened in accordance with centrally managed security policies. These include security baselines for operating systems, browsers and office applications, local firewalls, attack prevention rules, the controlled allocation and management of local administrator rights and the use of BitLocker.
20	Access to cloud services is governed by risk-based and context-sensitive access policies. Factors such as the user, the authentication method used and the management and security status of the terminal may be taken into account.

4.1.3 Data Usage Control

Measures ensuring that the persons entitled to use a data processing system can only access the data subject to their access authorisation, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

#	Measures
1	Unauthorised reading, copying, modification or deletion of data carriers is prevented by: ▪ Data carrier management. ▪ Software-related exclusion (authorisation concept). ▪ Secured interfaces.
2	Administrative activities are subject to documented guidelines regarding the separation of accounts, approval, logging and regular review.
3	The restriction of the access possibilities of the person entitled to use a computer system, exclusively to the data that is subject to his/her access authorisation, is ensured by: ▪ Automatic verification of the access authorisation by means of the user's credentials and additionally by two-factor authentication. ▪ User profiles according to the task area (need-to-know principle). ▪ The assignment, withdrawal and modification of authorisations (user administration) is comprehensible. ▪ Differentiated access authorisation to user programs. ▪ Differentiated processing options (read/change/delete). ▪ Limited administrative capabilities. ▪ Approval procedure for new users and for users when roles/task areas are changed (procedure). ▪ Removal of rights when employees leave the company. ▪ Privileged rights are granted in accordance with the principle of least privilege and, where technically feasible, are activated for a limited period of time. ▪ Separate administration accounts are used for administrative activities.
4	User and administrative rights are reviewed on a regular basis and as and when necessary, and assessed to determine whether they are still required. Any rights that are no longer required are revoked immediately.

4.1.4 Separation Rule

Measures for ensuring that data collected for different purposes can be processed separately.

#	Measures
1	Personal data may only be used for the purpose for which it was originally collected. Differentiated and separate processing is guaranteed by: ▪ Software-based exclusion (client separation). ▪ Database principle, separation via access regulation (authorisation concept). ▪ Separation of test and productive environments (two different systems). ▪ Separation of customer clients and of internal and customer data. ▪ Restriction or masking of personal test data.

4.2 Integrity (Article 32 para. 1 (b) GDPR)

4.2.1 Transfer Control

Measures ensuring that personal data cannot be illegally read, copied, altered or removed during electronic transmission or during its transport or storage on data carriers, and that it is possible to verify and ascertain the places to which a transmission of personal data is provided for by data transmission facilities.

#	Measures
1	As a general rule, data carriers are not dispatched.
2	Magnetic data carriers that are no longer needed are destroyed by repeated overwriting (withdrawal/deletion according to company specifications).
3	Laptops and data carriers are professionally deleted when sorted out.
4	Prohibition of the use of private data carriers.
5	Unauthorised reading, copying, modification or removal of data during transmission is prevented by: - OneDrive: Access activation through link to recipient via e-mail. - Credentials provided to customers for access; encryption of the data. - Completeness check as far as relevant. - Creation of an encrypted transport connection. - State-of-the-art encrypted transmission.
6	Controlled destruction of data carriers and paper documents in accordance with the DIN standard 66399.
7	Hard disk encryption: server and client systems.
8	For better support in analysis, installation, configuration and support services on the IT systems of the Customer, KUMAVISION uses the remote maintenance solution, TeamViewer. The above-mentioned services can be provided via the remote maintenance solution without having to go to the installation site of the respective IT systems. The Customer is responsible for the selection and provision of a remote maintenance solution. The Customer can, therefore, also use another remote maintenance solution instead of TeamViewer at any time. The Customer can make suggestions in this regard and describe its security requirements for remote maintenance access – e.g. in the form of a security concept. The set-up of the remote data connection is always activated for the respective session by the Customer. The responsibility for the IT security of the Customer's IT systems rests entirely with the Customer. If the remote maintenance is to be carried out directly by an approved subcontractor of KUMAVISION or by a third party, with the knowledge of the Customer without the involvement of KUMAVISION, a direct, independent contract data processing relationship shall arise between the Customer and the subcontractor, or third party, not involving the actual or legal responsibility of KUMAVISION. In this case, the Customer on the one hand, and the subcontractor or third party on the other, must conclude an agreement on the contract data processing under their own responsibility, for the admissibility under data protection law, the contractual framework conditions and also the technical and organisational measures to be used. Information on connection and data security, as well as instructions for installing and parameterising TeamViewer, can be found at https://www.teamviewer.com/en/documents. KUMAVISION uses two-factor authentication to log in to its TeamViewer accounts and uses the option to designate trusted devices in TeamViewer.
9	Protection against inadvertent data disclosure, for example through organisational and technical DLP measures.
10	External access only via secure connections/systems.
11	(Remote) maintenance procedure involving monitoring and logging only; the user can terminate the connection at any time.

4.2.2 Input Control

Measures ensuring that it is possible to subsequently verify and ascertain whether, and by whom, personal data has been entered, changed or removed in data processing systems.

#	Measures
1	Whether and by whom data has been entered in, changed or removed from DP systems can subsequently be verified and determined retrospectively by means of: ▪ User profiles. ▪ Logging via SIEM + Purview Audit. ▪ Logging of entered data (processing protocol). ▪ BC and other applications (CRM, SharePoint): created by and date of last change. ▪ Logging of failed logon attempts. ▪ Logging of administrative activities via the ticket system. ▪ Protection of logs against subsequent alteration. ▪ Role-based access to log data.
2	Where necessary and technically feasible, security-related events from identity, cloud, network and endpoint systems are logged centrally and correlated in a SIEM.
3	KUMAVISION AG collects, modifies or deletes personal data primarily within its own customer management systems (inventory and usage data). Further processing (change of purpose) of the data stored by the customer at KUMAVISION AG as part of the service provided (content data) does not take place.

4.3 Availability and Resilience (Article 32 para. 1 (b) and (c) GDPR)

Measures ensuring that personal data is protected against accidental destruction, loss or excessive use.

#	Measures
1	The data is protected against accidental destruction or loss, this being ensured by: ▪ Cloud systems with corresponding availability with a complete backup system. ▪ Incremental backups every 8 hours ▪ Daily backups with a 7-day retention period ▪ Weekly backups with a 4-week retention period ▪ Monthly backups on the last day of the month, with a 12-month retention period ▪ Annual backup on 31 December, with a 10-year retention period ▪ Fire and smoke alarm systems. ▪ Operation of an alarm system. ▪ Each task has its own server. ▪ Enhanced reliability for critical systems. ▪ Reconstruction of data sets (data backup concept) is ensured. ▪ Separation of backup data from production environment by cloud backup provider. ▪ Cloud providers' data centres with various certifications relating to availability. ▪ Back-up and recovery procedures are reviewed on a regular basis and the results are documented. ▪ Data recovery from backups is carried out regularly on a test basis to verify the effectiveness and usability of the backups. ▪ Protection of backups against being altered or deleted. ▪ Monitoring of failed backups. ▪ Capacity, availability and downtime monitoring.

4.4 Procedure for Regular Review, Assessment and Evaluation (Article 25 para. 1 GDPR; Article 32 para. 1 (d) GDPR)

4.4.1 Data Protection Management

KUMAVISION AG is supported by the German Data Protection Law Office (external Data Protection Officer, Maximilian Musch). The German Data Protection Law Office uses its own specially created data protection management system (DSMS), in which all the measures, procedures, activities, etc. in the area of data protection are mapped. The DSMS contains the most important legal data protection regulations and a comprehensive structure for mapping the data protection measures, and also includes an action plan for the legally compliant implementation of the EU Data Protection Regulation (accountability according to Art. 5 para. 2 GDPR).

In addition to fulfilling accountability, the DSMS also functions as an action plan for implementing and reviewing the necessary data protection measures. Regular control measures are derived from this and tracked via the DSMS as well as the internal work/status logs and audit reports. The DSMS is based on the DIN 27001 standard for information security and enables regular testing, assessment, evaluation and documentation of the measures.

4.4.2 Incident Response Management / Processes

A ticketing system is implemented for the immediate reporting of all types of incidents to IT. The user guideline documents processes and reporting channels with procedure and persons responsible. In addition, intrusion detection systems are used.

A managed security operations centre (managed SOC) is used to continuously monitor the IT security situation. Security-related incidents are recorded, analysed and assessed centrally. In the event of detected or suspected security incidents, an alert is triggered and the incident is handled in accordance with defined incident response processes.

In addition, internal processes for dealing with data protection/data security incidents, data privacy enquiries, the introduction of (new) data processing systems, a service provider/supplier management system, etc. have been implemented. Corresponding templates, documents to aid understanding as well as for documentation are also provided.

4.4.3 Privacy by Default Settings (Article 25 para. 2 GDPR)

In principle, only data that is appropriate and necessary for business purposes is collected and processed. Automated data collection and processing procedures are designed in such a way that only the necessary data is collected. For example, KUMAVISION AG is a service provider in the Microsoft Dynamics environment and is not responsible for the design of the product. KUMAVISION AG acts according to customer specifications with respect to the design, realisation, implementation and support of the system.

However, in order to use and design the systems in the most data-protection-compliant way possible, various tools, processes and documents are available to make it easier for the persons involved in the data processing to use the systems and data processing procedures in the most data-protection-compliant way possible. The external data protection officer is consulted as necessary during the system implementation and new data processing procedures.

4.4.4 Contract Data Control

Measures ensuring that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the client.

#	Measures
1	All the employees have been instructed in data protection, are committed to maintaining data secrecy, and have accepted the respective confidentiality and non-disclosure agreements as an integral part of their employment contract.
2	Detailed information exists regarding the purpose, nature and extent of the commissioned processing and use of the personal data of the client pursuant to Art. 28 GDPR. The relevant information is contractually agreed.
3	The service provider has, where necessary, appointed a company data protection officer and ensures, through the data protection organisation, that this officer is appropriately and effectively integrated into the relevant operational processes.
4	A regular examination of the commissioned service providers is carried out and documented by its own data protection officer, the information security officer or the internal IT administration. These examinations also take place on site, as applicable.
5	Critical service providers and cloud providers are regularly audited with regard to their technical and organisational security measures. In this regard, particular consideration is given to certifications, audit reports and other appropriate evidence.
6	Verbal orders must be confirmed in writing and documented.
7	Individual orders are only awarded by named contact persons.
8	Only restrictive access rights are granted to the relevant technical environments. If the system is accessed externally, the access will be deactivated or disabled after termination of the collaboration.

4.5 Pseudonymisation and Encryption (Article 32 para. 1 (a) GDPR)

Pseudonymisation procedures are possible in principle but are the responsibility of the Customer during data processing and are not part of the original service of KUMAVISION AG.

Appropriate encryption systems are implemented for data carriers and mobile terminals (BitLocker encryption). Encryption technologies are also used for the transmission of data. A Directive shall apply for the handling of (mobile) data carriers. Restrictive access rights also apply for accessing servers / test databases / development system, etc.

4.6 ISO/IEC 27001:2022 Certification

KUMAVISION AG is certified according to the ISO/IEC 27001 standard in the scope of "Development, Implementation and Support of customized industry-specific Software Solutions combined with Consulting for business process digitalization" and operates an information security management system.

The current certificate can be found here: <https://kumavision.com/en/zertifizierungen>

4.7 External Data Protection Officer

External Data Protection Officer of KUMAVISION AG according to Art. 37 General Data Protection Regulation (GDPR) or Section. 38 para. 1 BDSG (Federal Data Protection Act).

Maximilian Musch

Magister Artium (TU Darmstadt), certified, accredited Data Protection Officer (udis)

Maximilian Musch data protection consultancy
Brodmannstr. 1a
88090 Immenstaad
www.dsbmm.de

Contact: Data Protection Officer
Email: datenschutz@kumavision.com
Tel. +49 7542 / 94921-02