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

Date: July 2023
Author: Maximilian Musch – Deutsche Datenschutzkanzlei
Version: 4.3
Classification: public

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
3.4	Modifications	12.08.2019	DCO/DPO	Adaptation / amendment / transfer control und input control
3.5	Adaptations / updates	18.12.2020	IT	Adaptation / amendment
3.6	Revisions	29.12.2020	DCO	Adaptations / amendments
3.7	Review and amendment	10.02.2021	DPO	Amendment / adaptation
4.0	Release		DCO	Examination and release
4.1	Adaptations / updates	20.07.2022	DCO	Amendment / integritiy transfer control
4.2	Adaptations / updates	24.07.2023	DPO / IT	Reference to ISO 27001 certification Adaption Contract Data Control Amendment Entry Control, Transfer Control and Availability
4.3	Current CI	25.07.2023	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 Art.38 para.1 BDSG-neu (Federal Data Protection Act, new.) Those employed in the data processing are committed in writing to maintaining data secrecy as well as confidentiality. The Data Protection Officer and the data protection coordination 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, 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 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. The subcontractors are carefully selected and reviewed with respect to their safety awareness and expertise.

Some safeguards of the following checklist, relating to this section, are not indicated separately, because they lie within the responsibility of the subcontractors, or they are not published in detail for reasons of maintaining safety 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

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

#	Measures
1	The access control to the server rooms is ensured by the spatial structure of the respective computer centre and the control systems used there (restrictive, documented, double access authorisation procedure:- card and key; locked doors; Intruder Alarm System: additional card to disarm the system; the IT administration, exclusively, is permitted access).
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 / entrance 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	There is a central visitor reception. The offices are only accessible via this reception.
10	An alarm system secures the computer centre from unauthorised access, also outside business hours.
11	Security and surveillance duty:- switching on the burglar alarm system (computer centre).
12	The archive is similarly locked and may only be accessed by authorised employees (management, accounting).
13	Visitors are only permitted to remain on the business premises when accompanied by an employee. Maintenance services and visitors to the data centre are constantly monitored/escorted.
14	Video surveillance (locations:- Dortmund, Markdorf, Nürnberg, Stuttgart)
15	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.

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 to a minimum of the persons with authorised access.
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 as to IT services. Registration is exclusively possible over registered user accounts and password. For external access a second factor for registration is also required.
5	The guest WLAN is separated from the actual system (guest WLAN agreement with password).
6	A policy is available with specifications for the password standard.
7	A clear assignment of user accounts to users is possible.
8	Admin and User are clearly assigned by name.
9	Use of firewalls and intrusion detection systems for the prevention and detection of attacks.
10	State-of-the-art firewalls (restrictive from outside to inside; ports are closed).
11	A password policy is implemented with a sufficient standard of protection (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); change (once a year); reporting channels in the case of a third party being suspected of knowing the password; replacing initial/one-time passwords after first use; deactivating the "Remember/Save password" function.
12	Spam filters and virus-protection programmes (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.
13	Use of a central spam filter (central input email). Emails are marked and forwarding is prevented, if applicable. Use of automatic updates and signature recognition.
14	Automatic screen locks when leaving the workstation (password-protected) are controlled by an internal policy.
15	Functional restriction of the use of workplaces (restrictive allocation of rights according to function / activity).
16	Use of firewall- and network-policy (i.a. use of WLAN in the corporate network).
17	Hard disk encryption is used (BitLocker).
18	Patch Management Automated distribution of updates and patches of software within the company. Updates / patches cannot be bypassed, and/or they are automated. Only released patches / updates can be installed.
19	Carrying out penetration tests to check the security architecture and the measures used.
20	Automatic logout from systems in the case of a longer period of inactivity.

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, changing or deleting of data carriers is prevented by: ▪ Data Carrier Management. ▪ Use of external data carriers (customers) only in exceptional cases in a separate development environment. ▪ Software-related exclusion (authorisation concept). ▪ Secured interfaces.
2	The restriction of the access possibilities of the person entitled to use a computer system, exclusively to the data that are subject to his access authorisation, is ensured by: ▪ Automatic verification of the access authorisation by means of the user's credentials and, in the case of MS365 applications, by two-factor authentication. ▪ User profiles according to the task area (need-to-know principle). ▪ Exclusive menu control depending on the authorisation. ▪ The assignment, withdrawal and modification of authorisations (user administration) is comprehensible. ▪ Differentiated access authorisation to user programmes. ▪ Differentiated processing options (read / change / delete). ▪ Limited domain functions. ▪ Approval procedure for new users and for users when roles/task areas are changed (procedure).
3	Management of an administration concept (without gradations).
4	A concept for drive usage and allocation exists (AD-technical access to shared directories).

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 they were originally collected. The differing and separate processing is guaranteed by: ▪ Software-based exclusion (client separation). ▪ Database principle, separation via access regulation (authorisation concept). ▪ Separation of test and productive data (two different systems). ▪ Separation of functions ▪ Separation of development and production programmes (two different Active Directories).

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 their 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	Data carriers are only dispatched in exceptional cases. Dispatched data carriers are protected by passwords. Migration, if applicable, for customers (hard disk comes from customers).
2	Magnetic data carriers that are no longer needed are destroyed by repeated overwriting (withdrawal / deletion according to company specifications).
3	The documents and data storage media are disposed of and destroyed appropriately for ensuring the required protection. Servers are destroyed or deleted according to specification (certification by external service providers).
4	Notebooks and data carriers are deleted professionally when sorted out.
5	Prohibition of the use of private data carriers.
6	Unauthorised reading, copying, modification or removal of data during transmission is prevented by: ▪ OneDrive: Access activation through link to recipient via e-mail. ▪ Access data to customer for access; encryption of the data. ▪ Completeness check as far as relevant. ▪ Creation of an encrypted transport connection.
7	The transfer of personal data takes place by using the following services: ▪ Regularly WWW (https, VPN). ▪ Other services and transport methods that fulfil the desired purpose and the current level of security technology in a satisfactory or better way (FTP server in connection with password-protected ZIP files).
8	Controlled destruction of data carriers and paper documents in accordance with the DIN standard 66399 with security level 4.
9	Protected entrance for delivery and pick-up.
10	Hard disk encryption: Client systems.
11	For better support in analysis, installation, configuration and support services on the IT systems of the client, 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 client is responsible for the selection and provision of a remote maintenance solution. The client can, therefore, also use another remote maintenance solution instead of TeamViewer at any time. The client 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 client. The responsibility for the IT security of the client's IT systems rests entirely with the client. 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 order 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 on 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 the connection and data security, as well as instructions for the installation and parameterisation of TeamViewer can be found at https://www.teamviewer.com/de/dokumente. KUMAVISION uses two-factor authentication to log in to its TeamViewer accounts and uses the option to designate trusted devices in TeamViewer.
12	External access only via secure connections/systems. VPN access for mobile workstations/home offices.

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: ▪ User profiles. ▪ User identification. ▪ Logging via Active Directory. ▪ Firewall logging (TCP / IP). ▪ Logging of entered data (processing protocol). ▪ NAVISION and other applications (CRM, Sharepoint):- Creator and last modification. ▪ Logging of failed logon attempts. ▪ Logging of administrative activities via the Ticket System.
2	KUMAVISION AG collects, changes 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 are protected against accidental destruction, loss or excessive use.

#	Measures
1	The data are protected against accidental destruction or loss, this being ensured by the ▪ Use of RAID hard disk systems as well as cloud systems with corresponding availability with a complete backup system. ▪ Overnight security of the entire system. ▪ Use of UPS: Shutdown systems: Cache stores data. ▪ Fire and smoke alarm systems. ▪ Operation of an alarm system. ▪ Use of air conditioning with room-temperature monitoring. ▪ Exclusion on the software side:- distribution of the servers for independent and autonomous task execution (shared-nothing architecture). ▪ Each task has its own server. ▪ Multiple incremental database and system backups (full overnight backup). ▪ Backups according to a time schedule that adequately reflects the changes in the data through usage. ▪ Reconstruction of data stocks (data-backup concept) is ensured. Separation of backup data from production environment by cloud backup provider. ▪ Daily backup with 33 days provision. ▪ Monthly backup with 12 months provision.

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

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 for a better 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 are collected and processed that are appropriate and necessary for business purposes. Methods of automated data collection and processing are structured such, that only the required data are 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.
3	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.
4	The service provider has if necessary, appointed a company data-protection officer and due to the data protection organisation, ensures the appropriate and effective integration thereof into the relevant operational processes.
5	A regular examination of the commissioned service providers is carried out and documented by its own data protection officer, the IT security officer, or the internal IT administration. These examinations also take place on site, as applicable.
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)

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..

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

4.6 Certification ISO/IEC 27001:2013

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 Art. 38 para. 1 BDSG-neu (Federal Data Protection Act, new).

Maximilian Musch
Magister Artium (TU Darmstadt), certified, accredited Data Protection Officer.

Deutsche Datenschutzkanzlei
Office (Büro) Lake Constance
Richard-Wagner-Str. 2, 88094 Oberteuringen
www.deutsche-datenschutzkanzlei.de

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