Technical/organisational measures within the DKV Mobility Group

Version 1.4	Status: 24.11.2023
Department responsible for the subject matter:	DKV / Data Protection Officer
Language version:	EN

Proof of change

Version	Date	Editor	Section	Reason for the change
0.1	04.02.2015	Andreas Erle	All	First version in new form
1.0	04.02.2016	Andreas Erle	All	Annual audit
1.1	06.10.2017	Andreas Erle	All	Adaptation to EU-DSGVO
1.2	20.10.2017	Andreas Erle	2.2; 2.4; 2.10; 2.15; 2.16; 2.17; 2.18	Adaptation to EU-DSGVO
1.3	01.09.2020	Andreas Erle	All	Updates
1.4	19.11.2021	Andreas Erle	All	Updates
1.5	24.11.2023	Andreas Erle	All	Updates

Test report

This document must be reviewed and, if necessary, updated at least once a year, i.e. within a period of one month from the entry into force or the last amendment of the Directive.

Date (entry into force or latest amendment)	Earliest test date	Latest test date	Competent body	Comment
24.11.2023	*01.11.2024*	*30.11.2024*	*Data Protection Officer*	

Table of Contents

1. Subject matter and objective

Within the framework of the correct implementation of the processing of personal data in accordance with data protection law, the technical and organisational measures that are necessary must be taken in accordance with Article 32 of the EU General Data Protection Regulation (EU GDPR), as long as their expense is in reasonable proportion to the intended protective purpose.

This document describes the technical and organisational measures implemented in the companies of the DKV Mobility Group.

The description is based on Section 64 of the new Federal Data Protection Act (valid from 25 May 2018), well aware that this section is not relevant for non-public bodies, as DKV does not fall within the scope of Part Three of the Act. However, the description according to the requirements of the new BDSG is more detailed than the requirements of the EU General Data Protection Regulation. For a better illustration of the compliance with the requirements of the technical and organisational measures according to the requirements of the EU Data Protection Regulation, an overview with a mapping was created, which shows the allocation between the new BDSG and the EU Data Protection Regulation. The overview can be found in the appendix of this document.

2. Technical and organisational measures

2.1 Access control

The objective of access control is to prevent *unauthorised persons from gaining* access to processing equipment with which processing is carried out.

2.1.1 (ZGK1) Access control system

The company headquarters is secured by an access control system. Employees are issued with a personalised access card with which they have access to the individual access areas (office zones, individual offices, special security areas). These cards are issued centrally and blocked directly in the system if the employee is lost or leaves.

2.1.2 (ZGK2) Key issue/management

Certain sensitive areas are additionally secured with keys. Each key is issued centrally, documented by means of a key issue log and countersigned on an electronic signature pad.

2.1.3 (ZGK3) Reception/interaction with visitors/service providers

Visitors must be registered at the reception desk on the ground floor of the company's headquarters and are then issued with a visitor's badge upon arrival against signature and registration. This does not allow independent access to office areas. Visitors may only move through the building accompanied by an employee of DKV Mobility Group.

Visitors who park in the designated visitor parking spaces and reach reception from the underground car park can contact reception via a camera-based call system and are then guided through the stairwell to reception.

Service providers must be registered at the reception desk on the ground floor of the company's headquarters and are then issued with a service provider ID card upon arrival against signature and registration. This only allows access to office areas defined in advance.

2.1.4 (ZGK4) Monitoring equipment

Outside the operating hours of the building, it is secured by a burglar alarm system, which, when triggered, carries out a direct alarm.

The arming of the burglar alarm system takes place by a security service, which additionally carries out regular control rounds.

2.2 Data medium control

The aim is to prevent unauthorized reading, copying, modification or deletion of data carriers.

2.2.1 (DTK1) Inventory

All data carriers in the company infrastructure are inventoried.

2.2.2 (DTK2) Encryption

The storage of personal data on mobile devices or USB data carriers is carried out in encrypted form.

2.2.3 (DTK3) Destruction of data carriers and paper

Data carriers are physically deleted before they are used again. Data carriers to be discarded and defective data carriers are destroyed and logged in accordance with DIN 66399 in compliance with data protection level 4.

The destruction of paper with personal content is also carried out in accordance with DIN 66399 security level 4. The documents are collected in locked bins, which are regularly collected by a certified service provider. The destruction is logged by the service provider.

2.3 Memory Control

The aim is to prevent the unauthorised entry of personal data and the unauthorised disclosure, modification and deletion of stored personal data.

2.3.1 (SPK1) Password procedure

The workstation systems are protected by passwords, the assignment of which, the requirements for their design, validity periods, etc. are defined in a password policy (within the framework of the security specifications).

The workstation systems lock automatically after a set period of time.

2.3.2 (SPK2) User master records

Each employee has his or her own user master record, which is then used to regulate access to personal data as part of access control. The disclosure of access data and the associated passwords to other employees is prohibited.

2.4 User control (BEK1)

The aim is to prevent the use of automated processing systems by unauthorised persons with the aid of data transmission equipment.

2.4.1 (BEK1) Authentication

Access to processing systems integrated in the company is only possible by authorized persons and devices. Users must authenticate for network access. Access to the company network is only permitted through company-owned devices. All mobile devices (smartphones, tablets, etc.) are integrated into a mobile device management.

If an employee leaves, the corresponding user accounts of the employee are immediately deactivated so that no further accesses can take place.

2.4.2 (BEK2) Firewall

Local systems in the company are equipped with software firewalls. In addition, hardware firewalls are used for the network connection to the outside. The firewall settings are regularly checked and updated.

2.4.3 (BEK2) Remote maintenance

Remote maintenance access is used at various points in the company. However, these are only activated when required and deactivated again once the work has been completed.

2.5 Access control

The aim is to ensure that those authorised to use an automated processing system have access only to the personal data covered by their access authorisation.

2.5.1 (ZGK1) Password-based access control

Access to the workstation systems and applications is controlled by passwords. The assignment of authorizations, the requirements for their design, validity periods, etc. are defined in writing by the department.

2.5.2 (ZGK2) Separate user master records

Each employee has his or her own user master record for each system that processes personal data, which is then used to regulate the authorizations for accessing personal data as part of access control. The disclosure of access data and the associated passwords to other employees is prohibited.

2.5.3 (ZGK3) Differentiated authorizations

Access to personal data is regulated by personal user accounts and the authorizations assigned to these user accounts or the roles assigned to these user accounts.

The assignment of authorizations is carried out and documented as part of an employee connection process for new employees (and also for existing employees if changes are made).

When an employee leaves, a corresponding process ensures the revocation of authorizations, deactivation and subsequent deletion of user accounts.

2.6 Transmission control

The aim is to ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available by means of data communication equipment.

2.6.1 (UGK1) Logging

The transfer of personal data to the external service providers (card minting, dispatch) is logged. The logs are checked for plausibility and correctness at regular intervals.

2.7 Input control

The aim is to ensure that it is possible to verify and establish ex post which personal data have been entered or modified in automated processing systems, at what time and by whom.

2.7.1 (ECC1) Logging

Creation of and changes to personal data in the systems are logged by means of corresponding log files or change notices on the corresponding objects.

Unauthorized attempts to access the systems are also logged by the system and regularly evaluated.

2.8 Transport control

The aim is to ensure that the confidentiality and integrity of personal data are protected during the transmission of personal data and during the transport of data media.

2.8.1 (TK1) Encryption/Tunnel connection

The transfer of personal data to partners is carried out by means of closed networks or, in the case of transfer via the Internet, in a secured form (by means of encrypted VPN tunnels).

The storage of personal data on mobile devices or USB data carriers is carried out in encrypted form.

2.8.2 (TK2) Mobile devices/external data carriers

For the hard disks of the company notebooks, encryption software is used that requires decryption with user-specific access data before the operating system is started (preboot authentication).

The use of USB data carriers is limited to certain models; the data on these data carriers is automatically encrypted when used on a company computer.

2.9 Recoverability

The goal is to ensure that deployed systems can be restored in the event of a failure.

2.9.1 (WHBK1) Emergency plan

The service providers used to carry out the processing of personal data have documented emergency procedures that are regularly reviewed and tested.

2.10 Reliability

The aim is to ensure that all functions of the system are available and that any malfunctions that occur are reported.

2.10.1 (ZVL1) Monitoring

To ensure the reliability of the systems, they are monitored. The networks are also affected by this in order to be able to guarantee data transmission within the networks.

2.10.2 (ZVL2) Statistics

Statistics are kept to prove reliability. Failure rate statistics as well as availability statistics are maintained through various key figures.

2.11 Data integrity

The aim is to ensure that stored personal data cannot be damaged by system malfunctions or that this can be detected.

2.11.1 (DI1) Checksums

The integrity of the transmitted personal data is monitored by checksums.

2.12 Order control

The aim is to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

2.12.1 (ATK1) Clear contract design

If personal data is transferred to a service provider for processing on behalf of a third party, a standard contract for commissioned data processing is concluded with the service provider in accordance with Art. 28 EU-DSGVO. This contract contains the type of personal data transferred for processing on behalf of the service provider, the purpose of the processing and the technical/organisational measures.

2.12.2 (ATK2) Control rights

In the contracts concluded with the processing service providers, the control rights that the contracting authority has are explicitly formulated.

2.12.3 (ATK3) Audits

If personal data is passed on to a service provider for processing on behalf of the company, then this service provider is regularly subjected to a data protection and information security audit. These audits are documented, any findings communicated and their remediation followed up.

2.13 Availability control

The aim is to ensure that personal data is protected against destruction or loss.

2.13.1 (VEK1) Backups

The productive systems are regularly backed up by the service provider. For the workstation systems, the libraries are backed up automatically; these backups, in turn, are also subject to the backup concept for the systems.

2.13.2 (VEK2) Redundancy of the systems

Personal data is processed in redundantly designed data centers of the external service providers. Regular tests are carried out as part of emergency and disaster planning.

2.13.3 (VEK3) RAID/hard disk mirroring

In the productive systems, the data is stored redundantly.

2.13.4 (VEK4) Uninterruptible power supply

The servers in the data centers are buffered via UPS systems, thus temporarily initiating operation in the event of a power supply failure or an orderly shutdown in such a case.

2.13.5 (VEK5) Fire protection

Fire protection detectors in the data centres are connected to a band alarm system (BMA) and automatically alert the fire brigade in the event of a fire.

2.13.6 (VEK6) Virus protection

Workstation systems are protected with virus protection that is automatically updated with the latest virus patches.

Server systems are protected - as far as technically possible - with virus protection that is automatically updated with current virus patterns.

2.14 Separability

The aim is to ensure that personal data collected for different purposes can be processed separately.

2.14.1 (TRK1) Separation of production and test systems

The processing of personal data is carried out in a separate system ("productive system"), the development and error analysis/remediation in another system ("test system").

2.14.2 (TRK2) Separation of personnel

The processing of personal data and the development in the systems are carried out by personnel who are physically and organisationally separated.

2.14.3 (TRK3) Commitment/training of employees

The employees are committed to data protection and data secrecy and are further sensitized in regular training courses.

2.14.4 (TRK4) Logical separation

Personal data is separated in the systems by logical properties such as clients, sales offices, (main) customers, and so on.

2.15 Memory limitation (data deletion) (SPG1)

The objective is to ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; personal data may be kept for longer periods if the personal data are processed solely for archiving purposes in the public interest or for scientific and historical research purposes, or for statistical purposes as referred to in Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation to protect the rights and freedoms of the data subject ('storage limitation')

Deletion concepts are available for systems and processes, in particular CRM and ERP systems as well as office communication.

2.16 Load capacity (BEL1)

The goal is to ensure that IT systems function properly even under high usage frequency (performance). The resilience of IT systems is fundamental for maintaining business operations, i.e. for business continuity.

Performance studies are performed by applying artificially generated load or load logged on comparable systems to a system. Resource utilization and response times are measured.

Redundant WAN connections are available in the company for protection, as well as sufficient dimensioning of storage systems and main memory in IT systems.

2.17 Sustainability (NHK1)

The aim is to ensure that the processing of personal data is guaranteed in the long term.

The formats for data backups are deliberately selected in the company in order to be able to guarantee a long-term backup and restore of data.

An orderly change management exists in the company. This means, for example, that updates are only installed after prior testing in order to avoid system failures due to new updates.

2.18 Regular evaluation of effectiveness (REW1)

The objective is to establish a procedure for periodic review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing.

The regular evaluation of the effectiveness of the technical and organisational measures is mapped by the DSMS and ISMS. In the CIP cycle, the TOMs are considered and reviewed for appropriateness for the company. Penetration tests and data back-up tests are regularly carried out in the IT infrastructure to ensure secure operation