Technisch/Organisatorische Maßnahmen innerhalb der DKV Mobility Group

Version 1.5	Stand: 24.11.2023
Fachlich zuständige Stelle:	DKV / Datenschutzbeauftragter
Sprachversion:	DE

Änderungsnachweis

Version	Datum	Bearbeiter	Abschnitt	Grund der Änderung
0.1	04.02.2015	Andreas Erle	Alle	Erste Version in neuer Form
1.0	04.02.2016	Andreas Erle	Alle	Jährliche Prüfung
1.1	06.10.2017	Michael Schröder	Alle	Anpassung an EU-DSGVO
1.2	20.10.2017	Michael Schröder	2.2; 2.4; 2.10; 2.15; 2.16; 2.17; 2.18	Anpassung an EU-DSGVO
1.3	01.09.2020	Andreas Erle	Alle	Aktualisierungen
1.4	19.11.2021	Andreas Erle	Alle	Aktualisierungen
1.5	23.11.2023	Andreas Erle	Alle	Aktualisierungen

Prüfprotokoll

Diese Dokument muss mindestens einmal jährlich, d. h. innerhalb eines Zeitraums von einem Monat ab Inkrafttreten bzw. letzter Änderung der Richtlinie, überprüft und ggf. aktualisiert werden.

Datum (Inkrafttreten bzw. letzte Änderung)	Frühester Prüftermin	Spätester Prüftermin	Fachlich zuständige Stelle	Bemerkung
24.11.2023	*01.11.2024*	*30.11.2024*	*Datenschutz-beauftragter*	

Inhaltsverzeichnis

1. Gegenstand und Ziel

Im Rahmen der datenschutzrechtlich korrekten Durchführung der Verarbeitung personenbezogener Daten sind gemäß Art. 32 EU-Datenschutz-Grundverordnung (EU-DSGVO) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, solange ihr Aufwand in angemessenem Verhältnis zu dem angestrebten Schutzzweck steht.

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die in den Unternehmen der DKV Mobility Group umgesetzt werden.

Die Beschreibung orientiert sich an § 64 des neuen Bundesdatenschutzgesetztes (Gültigkeit ab 25. Mai 2018), wohl wissentlich, dass dieser Paragraph für nicht-öffentliche Stellen nicht relevant ist, da die DKV nicht in den Anwendungsbereich des dritten Teils des Gesetzes fällt. Die Beschreibung nach den Vorgaben des neuen BDSG ist jedoch ausführlicher als die Anforderungen der EU-Datenschutz-Grundverordnung beschrieben. Zur besseren Veranschaulichung über die Einhaltung der Vorgaben der technischen und organisatorischen Maßnahmen nach den Vorgaben der EU-DSGVO wurde eine Übersicht mit einem Mapping erstellt, welche die Zuordnung zwischen neuem BDSG und EU-DSGVO zeigt. Die Übersicht befindet sich im Anhang dieses Dokuments.

2. Technische und organisatorische Maßnahmen

2.1 Zugangskontrolle

Das Ziel der Zugangskontrolle ist es, Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, zu verwehren.

2.1.1 (ZGK1) Zugangskontrollsystem

Der Firmensitz ist durch ein Zugangskontrollsystem abgesichert. Mitarbeiter bekommen eine personalisierte Zugangskarte, mit der sie Zugang zu den einzelnen Zugangsbereichen (Bürozonen, Einzelbüros, spezielle Sicherheitsbereiche) haben. Diese Karten werden zentral ausgegeben und bei Verlust oder Ausscheiden des Mitarbeiters direkt im System gesperrt.

2.1.2 (ZGK2) Schlüsselausgabe/-verwaltung

Bestimmte sensitive Bereiche sind zusätzlich mit Schlüsseln gesichert. Die Ausgabe eines jeden Schlüssels wird zentral vorgenommen, mittels eines Schlüsselausgabeprotokolls dokumentiert und auf einem elektronischen Unterschriften-Pad gegengezeichnet.

2.1.3 (ZGK3) Empfang/Umgang mit Besuchern/Dienstleistern

Besucher müssen am Empfang im Erdgeschoss des Firmensitzes angemeldet werden und bekommen dann nach Ankunft gegen Unterschrift und Registrierung einen Besucherausweis ausgehändigt. Dieser erlaubt keinen selbständigen Zugang zu Bürobereichen. Besucher dürfen sich nur begleitet von einem Mitarbeiter der DKV Mobility Group durch das Gebäude bewegen.

Besucher, die auf den ausgewiesenen Besucherparkplätzen parken und aus der Tiefgarage zum Empfang gelangen, können den Empfang durch eine kameragestützte Rufanlage kontaktieren und werden dann durch das Treppenhaus zum Empfang geführt.

Dienstleister müssen am Empfang im Erdgeschoss des Firmensitzes angemeldet werden und bekommen dann nach Ankunft gegen Unterschrift und Registrierung einen Dienstleisterausweis ausgehändigt. Dieser erlaubt nur Zugang zu im Vorfeld definierten Bürobereichen.

2.1.4 (ZGK4) Überwachungseinrichtungen

Außerhalb der Betriebszeiten es Gebäudes wird dieses durch eine Einbruchmeldeanlage gesichert, die bei Auslösung eine direkte Alarmierung durchführt.

Die Schärfung der Einbruchmeldeanlage findet durch einen Sicherheitsdienst statt, der zusätzlich regelmäßige Kontrollgänge durchführt.

2.2 Datenträgerkontrolle

Das Ziel ist die Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

2.2.1 (DTK1) Inventarisierung

Sämtliche Datenträger in der Unternehmensinfrastruktur sind inventarisiert.

2.2.2 (DTK2) Verschlüsselung

Die Speicherung personenbezogener Daten auf mobilen Endgeräten oder USB-Datenträgern erfolgt in verschlüsselter Form.

2.2.3 (DTK3) Vernichtung von Datenträgern und Papier

Datenträger werden vor der erneuten Verwendung einer physischen Löschung unterzogen. Auszusondernde und defekte Datenträger werden gemäß DIN 66399 datenschutzkonform nach Sicherheitsstufe 4 vernichtet und protokolliert.

Die Vernichtung von Papier mit personenbezogenem Inhalt wird ebenfalls gemäß DIN 66399 Sicherheitsstufe 4 vorgenommen. Die Sammlung der Dokumente findet in abgeschlossenen Tonnen statt, welche regelmäßig durch einen zertifizierten Dienstleister abgeholt werden. Die Vernichtung wird durch den Dienstleister protokolliert.

2.3 Speicherkontrolle

Das Ziel ist die Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

2.3.1 (SPK1) Kennwortverfahren

Die Arbeitsplatzsysteme sind durch Kennwörter geschützt, deren Vergabe, die Anforderungen an deren Ausgestaltung, Gültigkeitszeiträume etc. in einer Passwortrichtlinie (im Rahmen der Sicherheitsvorgaben) festgelegt sind.

Die Arbeitsplatzsysteme sperren sich nach einen festgelegten Zeitraum automatisch.

2.3.2 (SPK2) Benutzerstammsätze

Jeder Mitarbeiter besitzt einen eigenen Benutzerstammsatz, über den dann im Rahmen der Zugriffskontrolle der Zugriff auf personenbezogene Daten reguliert wird. Die Weitergabe der Zugangsdaten und der zugehörigen Passwörter an andere Mitarbeiter ist untersagt.

2.4 Benutzerkontrolle (BEK1)

Das Ziel ist die Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

2.4.1 (BEK1) Authentifizierung

Der Zugriff auf im Unternehmen integrierte Verarbeitungssysteme ist nur durch autorisierte Personen und Geräte möglich. Benutzer müssen sich für Netzwerkzugriffe authentifizieren. Der Zugriff auf das Firmennetzwerk ist nur durch firmeneigene Geräte gestattet. Alle mobilen Geräte (Smartphones, Tablets, usw.) sind in ein Mobile Device Management integriert.

Scheidet ein Mitarbeiter aus werden die entsprechenden Benutzerkonten des Mitarbeiters unverzüglich deaktiviert, dass keine weiteren Zugriffe erfolgen können.

2.4.2 (BEK2) Firewall

Im Unternehmen sind lokale Systeme mit Software-Firewalls ausgestattet. Zudem werden für die Netzwerkanbindung nach außen Hardware-Firewalls eingesetzt. Die Firewall-Einstellungen werden regelmäßig überprüft und aktualisiert.

2.4.3 (BEK2) Fernwartung

Im Unternehmen wird an verschiedenen Stellen mit Fernwartungszugängen gearbeitet. Diese werden jedoch nur bei Bedarf aktiviert und nach Abschluss der Arbeiten wieder deaktiviert.

2.5 Zugriffskontrolle

Das Ziel ist die Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

2.5.1 (ZGK1) Kennwortgestützte Zugriffskontrolle

Der Zugriff zu den Arbeitsplatzsystemen und Applikationen wird durch Kennwörter gesteuert. Die Berechtigungsvergabe, die Anforderungen an deren Ausgestaltung, Gültigkeitszeiträume etc. sind durch den Fachbereich schriftlich festgelegt.

2.5.2 (ZGK2) Separate Benutzerstammsätze

Jeder Mitarbeiter besitzt für jedes System, das personenbezogene Daten verarbeitet, einen eigenen Benutzerstammsatz, über den dann im Rahmen der Zugriffskontrolle die Berechtigungen für den Zugriff

auf personenbezogene Daten reguliert werden. Die Weitergabe der Zugangsdaten und der zugehörigen Passwörter an andere Mitarbeiter ist untersagt.

2.5.3 (ZGK3) Differenzierte Berechtigungen

Der Zugriff auf personenbezogene Daten wird durch personenbezogene Benutzerkonten und die auf diese Benutzerkonten vergebenen Berechtigungen beziehungsweise diesen Benutzerkonten zugewiesenen Rollen geregelt.

Die Vergabe der Berechtigungen wird im Rahmen eines Prozesses zur Mitarbeiteranbindung für neue (und bei Änderung auch für bestehende Mitarbeiter) vorgenommen und dokumentiert.

Bei Ausscheiden eines Mitarbeiters wird über einen entsprechenden Prozess der Entzug der Berechtigungen, die Deaktivierung und die darauf folgende Löschung der Benutzerkonten sichergestellt.

2.6 Übertragungskontrolle

Das Ziel ist die Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

2.6.1 (UGK1) Protokollierung

Die Übertragung personenbezogener Daten zu den externen Dienstleistern (Kartenprägung, Versand) wird protokolliert. Die Protokolle werden in regelmäßigen Abständen auf Plausibilität und Korrektheit geprüft.

2.7 Eingabekontrolle

Das Ziel ist die Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind

2.7.1 (EGK1) Protokollierung

Anlage und Änderungen personenbezogener Daten in den Systemen werden durch entsprechende Logdateien bzw. Änderungsvermerke an den entsprechenden Objekten protokolliert.

Ebenfalls werden systemseitig unberechtigte Zugriffsversuche auf die Systeme protokolliert und regelmäßig ausgewertet.

2.8 Transportkontrolle

Das Ziel ist die Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden

2.8.1 (TK1) Verschlüsselung/Tunnelverbindung

Die Übertragung personenbezogener Daten an Partnern erfolgt mittels geschlossener Netzwerke oder, im Falle der Übertragung über das Internet in gesicherter Form (mittels verschlüsselter VPN-Tunnel).

Die Speicherung personenbezogener Daten auf mobilen Endgeräten oder USB-Datenträgern erfolgt in verschlüsselter Form.

2.8.2 (TK2) Mobile Geräte/Externe Datenträger

Für die Festplatten der Firmennotebooks wird eine Verschlüsselungssoftware verwendet, die eine Entschlüsselung mit benutzerspezifischen Zugangsdaten vor dem Start des Betriebssystems erfordert (Preboot Authentication).

Die Verwendung von USB-Datenträgern ist auf bestimmte Modelle beschränkt, die Daten auf diesen Datenträgern werden bei Verwendung an einem Firmenrechner automatisch verschlüsselt.

2.9 Wiederherstellbarkeit

Das Ziel ist die Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

2.9.1 (WHBK1) Notfallplan

Die eingesetzten Dienstleister, die die Verarbeitung personenbezogener Daten durchführen, haben dokumentierte Notfallverfahren, die regelmäßig überprüft und getestet werden.

2.10 Zuverlässigkeit

Das Ziel ist die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

2.10.1 (ZVL1) Monitoring

Zur Sicherstellung der Zuverlässigkeit der Systeme werden diese gemonitort. Ebenfalls sind hiervon die Netzwerke betroffen, um die Datenübermittlungen innerhalb der Netze gewährleisten zu können.

2.10.2 (ZVL2) Statistiken

Zum Nachweis der Zuverlässigkeit werden Statistiken geführt. Durch verschiedene Kennzahlen werden Ausfallraten-Statistiken sowie Verfügbarkeits-Statistiken vorgehalten.

2.11 Datenintegrität

Das Ziel ist die Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können bzw. dass dies festgestellt werden kann

2.11.1 (DI1) Prüfsummen

Die Integrität der übertragenen personenbezogenen Daten wird durch Prüfsummen überwacht.

2.12 Auftragskontrolle

Das Ziel ist die Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

2.12.1 (ATK1) Eindeutige Vertragsgestaltung

Werden personenbezogene Daten zur Verarbeitung im Auftrag an einen Dienstleister weitergegeben, dann wird mit diesem ein Standard-Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 EU-DSGVO abgeschlossen. Dieser enthält die Art der zur Verarbeitung im Auftrag übergebenen personenbezogenen Daten, den Zweck der Verarbeitung und die technisch/organisatorischen Maßnahmen.

2.12.2 (ATK2) Kontrollrechte

In den Verträgen, die mit den Auftragsverarbeitungs-Dienstleistern abgeschlossen werden, sind die Kontrollrechte, die der Auftraggeber hat, explizit formuliert.

2.12.3 (ATK3) Audits

Werden personenbezogene Daten zur Verarbeitung im Auftrag an einen Dienstleister weitergegeben, dann wird dieser regelmäßig einem Datenschutz- und Informationssicherheitsaudit unterzogen. Diese Audits werden dokumentiert, eventuelle Findings kommuniziert und deren Behebung nachverfolgt.

2.13 Verfügbarkeitskontrolle

Das Ziel ist die Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

2.13.1 (VEK1) Backups

Die produktiven Systeme werden regelmäßig im Rahmen von Backups beim Dienstleister gesichert. Für die Arbeitsplatzsysteme werden die Bibliotheken automatisiert gesichert, diese Sicherungen wiederum unterliegen ebenfalls dem Backupkonzept der Systeme.

2.13.2 (VEK2) Redundanz der Systeme

Die Verarbeitung personenbezogener Daten erfolgt in redundant ausgelegten Rechenzentren der externen Dienstleister. Im Rahmen der Notfall- und Katastrophenplanung werden regelmäßige Tests durchgeführt.

2.13.3 (VEK3) RAID/Festplattenspiegelung

Bei den produktiven Systemen werden die Daten redundant gespeichert.

2.13.4 (VEK4) Unterbrechungsfreie Stromversorgung

Die Server in den Rechenzentren werden über USV-Anlagen gepuffert und so zeitweise der Betrieb bei Ausfall der Stromversorgung beziehungswiese das geordnete Herunterfahren in einem solchen Fall eingeleitet.

2.13.5 (VEK5) Brandschutz

Brandschutzmelder in den Rechenzentren sind auf eine Bandmeldeanlage (BMA) aufgeschaltet und alarmieren bei einem Brandfall automatisch die Feuerwehr.

2.13.6 (VEK6) Virenschutz

Arbeitsplatzsysteme werden mit einem Virenschutz, der automatisch durch aktuelle Virenpattern aktualisiert wird, geschützt.

Serversysteme werden – soweit technisch möglich – mit einem Virenschutz, der automatisch durch aktuelle Virenpattern aktualisiert wird, geschützt.

2.14 Trennbarkeit

Das Ziel ist die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

2.14.1 (TRK1) Trennung von Produktiv- und Testsystemen

Die Verarbeitung personenbezogener Daten wird in einem separaten System („Produktivsystem“) vorgenommen, die Entwicklung und Fehleranalyse/-behebung in einem anderen System („Testsystem“).

2.14.2 (TRK2) Trennung von Personal

Die Verarbeitung der personenbezogenen Daten und die Entwicklung in den Systemen werden von räumlich wie auch organisatorisch getrenntem Personal durchgeführt.

2.14.3 (TRK3) Verpflichtung/Schulung der Mitarbeiter

Die Mitarbeiter werden auf Datenschutz und Datengeheimnis verpflichtet und in regelmäßigen Schulungen weiter sensibilisiert.

2.14.4 (TRK4) Logische Trennung

Personenbezogene Daten werden in den Systemen über logische Eigenschaften wie Mandanten, Verkaufsbüros, (Haupt-) Kunden etc. getrennt.

2.15 Speicherbegrenzung (Datenlöschung) (SPG1)

Das Ziel ist die Gewährleistung, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“)

Für Systeme und Verfahren, insbesondere CRM- und ERP-System sowie Bürokommunikation liegen Löschkonzepte vor.

2.16 Belastbarkeit (BEL1)

Das Ziel ist die Gewährleistung, dass IT-Systeme auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß funktionieren (Performanz). Die Belastbarkeit der IT-Systeme ist grundlegend für die Aufrechterhaltung des Geschäftsbetriebs, also für die Business Continuity

Untersuchungen zur Performanz werden durch Anlegen künstlich erzeugter oder an vergleichbaren Systemen protokollierter Last an einem System durchgeführt. Hierbei werden die Ressourcennutzung und Reaktionszeiten gemessen.

Zur Absicherung sind redundante WAN-Anbindung im Unternehmen vorhanden sowie eine ausreichende Dimensionierung von Storage-Systemen und Arbeitsspeicher in IT-Systemen.

2.17 Nachhaltigkeit (NHK1)

Das Ziel ist die Gewährleistung, dass eine Verarbeitung der personenbezogenen Daten auf Dauer sichergestellt ist.

Die Formate für Datensicherungen werden im Unternehmen bewusst ausgewählt, um eine langfristige Sicherung und Rücksicherung von Daten gewährleisten zu können.

Im Unternehmen existiert ein geordnetes Changemanagement. Dies bedeutet beispielsweise, dass Updates nur nach vorherigem Test eingespielt werden, um keine Systemausfälle durch neue Updates zu erhalten.

2.18 Regelmäßige Evaluation der Wirksamkeit (REW1)

Das Ziel ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die regelmäßige Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen wird durch das DSMS sowie ISMS abgebildet. Im KVP-Zyklus werden die TOMs betrachtet und auf Angemessenheit für das Unternehmen überprüft. In der IT-Infrastruktur werden regelmäßig Penetrationstests und Datenrücksicherungstests durchgeführt, um einen gesicherten Betrieb gewährleisten zu können.

Anhang

TOMs Art. 32 DSGVO mit § 64 BDSG-neu verknüpft

		Pseudonymisierung / Verschlüsselung	Vertraulichkeit	Integrität	Verfügbarkeit	Belastbarkeit der Systeme	Verarbeitung auf Dauer	Wiederherstellbarkeit	Speicherbegrenzung	Regelmäßige Evaluation der Wirksamkeit
Nr.	§ 64 Abs. 3 DSAnpUG-EU	Art. 32 Abs. 1 lit. a DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. b DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. b DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. b DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. b DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. b DSGVO § 64 Abs. 2 Nr. 1 BDSG-neu	Art. 32 Abs. 1 lit. c DSGVO § 64 Abs. 2 Nr. 2 BDSG-neu	Art. 5 Abs. 1 lit. e DSGVO	Art. 32 Abs. 1 lit. d DSGVO
1	**Zugangskontrolle**		X							
2	**Datenträgerkontrolle**	X	X	X	X					
3	**Speicherkontrolle**	X	X	X	X					
4	**Benutzerkontrolle**	X	X	X	X					
5	**Zugriffskontrolle**	X	X	X	X					
6	**Übertragungskontrolle**	X		X	X					
7	**Eingabekontrolle**			X						
8	**Transportkontrolle**	X	X	X						
9	**Wiederherstellbarkeit**				X		X	X		
10	**Zuverlässigkeit**					X	X			X
11	**Datenintegrität**			X	X	X	X			
12	**Auftragskontrolle**		X	X						
13	**Verfügbarkeitskontrolle**			X	X	X	X			
14	**Trennbarkeit**		X	X						
15	**Speicherbegrenzung**						(X)		X	
16	**Belastbarkeit**				X	X				
17	**Nachhaltigkeit**						X			
18	**Regelmäßige Evaluation der Wirksamkeit**									X