Gemeindekassenverband Altenberge

Zweckverband der Gemeinden Altenberge, Laer und Metelen

Dienstanweisung
über den Datenschutz und die Datensicherheit
beim Gemeindekassenverband Altenberge
(DA Datenschutz)

Dienstanweisung über den Datenschutz und Datensicherheit

Für die Mitarbeiterinnen und Mitarbeiter des Gemeindekassenverbands Altenberge wird folgende

Dienstanweisung

erlassen:

1 Allgemeines

Das verfassungsrechtlich verankerte Recht auf informationelle Selbstbestimmung des Individuums ist im Zeitalter der heutigen Informationsgesellschaft in besonderem Maße schutzbedürftig. Technische und organisatorische Sicherheitsmaßnahmen sind daher unerlässlich, um sowohl eine effektive und bürgernahe Verwaltungsarbeit als auch eine zuverlässige Datenschutz- und Datensicherheitsstruktur zu gewährleisten.

Diese Dienstanweisung regelt für den Datenschutz im engeren Sinne sowie für die grundsätzlichen technischen und organisatorischen Maßnahmen des Datenschutzes die Zuständigkeiten und Aufgaben der Mitarbeiterinnen und Mitarbeiter des Gemeindekassenverbands Altenberge. Bestehende und künftige verwaltungsinterne Regelungen sind - soweit sie diesen Themenbereich betreffen - dieser Dienstanweisung anzupassen bzw. entsprechend anzuwenden.

Die Einhaltung der Gesetze und Verordnungen zum Datenschutz ist ein zentraler Bestandteil der dienstlichen Aufgabenerfüllung aller Mitarbeiterinnen und Mitarbeiter. Jede/r Bedienstete trägt die volle datenschutzrechtliche Verantwortung für die Ausübung seiner/ihrer Tätigkeit.

Der leichtfertige Umgang mit personenbezogenen Daten kann sowohl nachhaltige Schäden im Vertrauen der Bürgerinnen und Bürger als auch Schadenersatzforderungen sowie Disziplinar-, Bußgeld- und Strafverfahren zur Folge haben.

Der folgende Abschnitt 2 enthält allgemeine Anweisungen zum Datenschutz im engeren Sinn. Der Abschnitt 3 beschreibt die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes.

2 Datenschutz im engeren Sinne

2.1 Rechtsgrundlagen

Die wesentlichen Rechtsgrundlagen des Datenschutzes für die Kommunalverwaltungen in Nordrhein-Westfalen sind

- das Datenschutzgesetz des Landes Nordrhein-Westfalen (DSG NRW) vom 09.06.2000 in der jeweils gültigen Fassung,
- das Bundesdatenschutzgesetz (BDSG) vom 14.01.2003 in der jeweils gültigen Fassung (nur eingeschränkt) und
- spezialgesetzliche Regelungen des Bundes oder Landes mit vorrangiger Geltung.

2.2 Begriffsbestimmungen und sachlicher Geltungsbereich

2.2.1 Begriffsbestimmungen

Unter den Datenschutz fällt der gesamte Prozess der Verarbeitung personenbezogener Daten in Dateien und Akten. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person).

Die Datenverarbeitung besteht aus dem:

Erheben:	das Beschaffen von Daten über die betroffene Person
Speichern:	das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung
Verändern:	das inhaltliche Umgestalten gespeicherter Daten
Übermitteln:	das Bekannt geben personenbezogener Daten an einen Dritten durch Weitergeben, Gewähren der Einsichtnahme oder Gestatten des Abrufes in einem automatisierten Verfahren
Sperren:	das Verhindern weiterer Verarbeitung gespeicherter Daten
Löschen:	das Unkenntlichmachen gespeicherter Daten
Nutzen:	jede sonstige Verwendung personenbezogener Daten.

2.2.2 Sachlicher Geltungsbereich

Der Schutz personenbezogener Daten ist in sämtlichen Bereichen, die personenbezogene Daten selbst oder durch Einschaltung Dritter verarbeiten, zu gewährleisten. Er beschränkt sich nicht auf den Bereich der technischen Informationsverarbeitung.

2.3 Zuständigkeit

2.3.1 Mitarbeiterinnen und Mitarbeiter

Die Mitarbeiterinnen und Mitarbeiter haben bei der Ausübung ihrer dienstlichen Tätigkeit die Rechtsvorschriften über den Datenschutz zu beachten; sie tragen hierfür insoweit die unmittelbare Verantwortung.

Insbesondere ist es untersagt, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung der Beschäftigung beim Gemeindekassenverband Altenberge.

In Zweifelsfragen ist die Entscheidung der/des jeweiligen Vorgesetzten herbeizuführen.

2.3.2 Sachbereichsleiter/innen

Die Sachbereichsleiter/innen stellen die Beachtung der Rechtsvorschriften über den Datenschutz in ihrem Zuständigkeitsbereich sicher. Sie können hierzu besondere schriftliche Anweisungen treffen.

2.3.3 Behördliche/r Datenschutzbeauftragte/r

2.3.3.1 Bestellung

Der Verbandsvorsteher/Die Verbandsvorsteherin bestellt eine/n behördliche/n Datenschutzbeauftragte/n (DSB) und einen Vertreter/eine Vertreterin.

2.3.3.2 Rechtsstellung

Der/Die DSB ist dem Verbandsvorsteher/der Verbandsvorsteherin unmittelbar unterstellt und in dieser Funktion weisungsfrei.

Er/Sie hat ein Empfehlungsrecht in allen Fragen des Datenschutzes, jedoch kein Weisungsrecht gegenüber den einzelnen Organisationseinheiten. In streitigen Fällen entscheidet der Verbandsvorsteher/die Verbandsvorsteherin abschließend.

Er/Sie darf wegen der Erfüllung seiner/ihrer Aufgaben nicht benachteiligt werden.

Während seiner/ihrer Tätigkeit darf er/sie mit keiner Aufgabe betraut sein, deren Wahrnehmung zu Interessenkollisionen führen könnte.

2.3.3.3 Aufgaben

Der/Die DSB ist Ansprechpartner/in in allen Fragen des Datenschutzes für die Behördenleitung und die Mitarbeiterinnen und Mitarbeiter. Die Mitarbeiterinnen und Mitarbeiter können sich jederzeit in Angelegenheiten des Datenschutzes unmittelbar an den/die DSB wenden. Er/Sie ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf diese zulassen, verpflichtet, soweit er/sie von der betroffenen Person davon nicht befreit wurde.

Dem/Der DSB obliegen insbesondere folgende Aufgaben:

- Unterstützung der Kommunalverwaltung bei der Sicherstellung des Datenschutzes. Hierzu gehören die Beratung der Verwaltungsleitung und der Mitarbeiterinnen und Mitarbeiter in allen Fragen des Datenschutzes.
- Beratung der Daten verarbeitenden Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten. Hierzu gehört die Kooperation mit dem für den IT-Betrieb zuständigen Bereich.
- Vorabkontrolle und Überwachung der Einhaltung der Datenschutzvorschriften bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren zur Verarbeitung personenbezogener Daten.
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften bei der Erarbeitung behördeninterner Regelungen, wie z.B. Dienstvereinbarungen/-anweisungen, Richtlinien etc., und Maßnahmen zur Verarbeitung personenbezogener Daten.
- Vertrautmachen der mit Verarbeitung personenbezogener Daten befassten Personen mit den datenschutzrechtlichen Bestimmungen.

- Führung des Verfahrensverzeichnisses nach § 8 DSG NRW. Hierzu gehört die Gewährung der Einsicht in das Verzeichnis durch berechtigte Personen.
- Federführung in der Korrespondenz mit dem/der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen (LDI) und Prüfung ausgesprochener Empfehlungen und Beanstandungen des/der LDI.
- Überwachung der Fachbereiche auf die Einhaltung der Vorgaben zu Datenschutz und Datensicherheit; hierzu gehören auch unangemeldete Kontrollen und Stichproben.

Stellt die/der DSB Verstöße gegen die Vorgaben zu Datenschutz und Datensicherheit fest, kann sie/er diese beanstanden. Mit der Beanstandung können Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

2.4 Unterrichtung der Mitarbeiter/innen über den Datenschutz

Die Mitarbeiter/Die Mitarbeiterinnen sind vor dem Beginn ihrer Beschäftigung über die zu beachtenden Vorschriften zu unterrichten. Neben der allgemeinen Verpflichtung bei der Einstellung sollen sie zusätzlich durch die Fachbereichsleiter/innen über die in ihrem Tätigkeitsbereich zu beachtenden Vorschriften unterrichtet werden.

2.5 Verarbeitung personenbezogener Daten im Auftrag (§ 11 DSG NRW)

Bei der Verarbeitung personenbezogener Daten im Auftrag gem. § 11 DSG NRW ist der Gemeindekassenverband Altenberge für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich. Die Auswahl des Auftragnehmers hat unter besonderer Berücksichtigung der Eignung für die Gewährleistung der nach § 10 DSG NRW notwendigen technischen und organisatorischen Maßnahmen sorgfältig zu erfolgen. Der Auftrag ist schriftlich zu erteilen.

Darin ist der Auftragnehmer insbesondere auf den Umfang des Auftrages, die Datenschutzbestimmungen, seine Rechte und Pflichten und etwaige Schadensersatzregelungen hinzuweisen. Zudem ist ggf. eine Verpflichtung des Auftragnehmers nach dem Verpflichtungsgesetz vorzunehmen.

Die Auftragsunternehmen sollten so ausgewählt werden, dass auf sie die Vorschriften des DSG NRW Anwendung finden. Anderenfalls ist sicherzustellen, dass das Auftragsunternehmen die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle der/s LDI unterwirft (§ 11 Abs. 3 DSG NRW). Bei einer Auftragsdurchführung außerhalb DSG NRW ist sicherzustellen, dass die zuständige Datenschutzkontrollbehörde unterrichtet wird.

2.6 Grundsätze des Datenschutzes im engeren Sinne

2.6.1 Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur und ausschließlich dann zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die betroffene Person eingewilligt hat.

Die Einwilligung hat grundsätzlich schriftlich zu erfolgen, sie kann durch eine elektronische Form ersetzt werden, wenn

- sie nur durch eine eindeutige und bewusste Handlung der handelnden Person erfolgen kann,
- sie nicht unerkennbar verändert werden kann,
- ihr Urheber erkannt werden kann,
- die Einwilligung bei der verarbeitenden Stelle protokolliert wird und
- der betroffenen Person jederzeit Auskunft über den Inhalt ihrer Einwilligung gegeben werden kann.

2.6.2 Allgemeine Regeln für die Datenverarbeitung

Der Datenschutz erfordert, dass

- personenbezogene Daten grundsätzlich bei der betroffenen Personen mit ihrer Kenntnis erhoben werden,
- personenbezogene Daten grundsätzlich nur für die Zwecke weiterverarbeitet werden, für die sie erhoben worden sind,
- nur Befugte personenbezogene Daten zur Kenntnis nehmen,
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können,
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat,
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben,
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können,
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, so dass sie in zumutbarer Zeit nachvollzogen werden können, und
- personenbezogene Daten nur soweit erforderlich und möglichst sparsam verarbeitet werden.

2.7 Verstöße gegen den Datenschutz im engeren Sinne

Die Mitarbeiterinnen und Mitarbeiter sind für die Folgen ihrer Handlungen verantwortlich, die zu einer Verletzung der Sicherheit bzw. des Schutzbedarfs personenbezogener Daten führen könnten oder bereits geführt haben.

Als Verstöße gelten insbesondere beabsichtigte oder grob fahrlässige Handlungen, die

- der Verwaltung durch Gefährdung der Sicherheit von Daten einen tatsächlichen oder drohenden finanziellen Verlust einbringen,
- den unberechtigten Zugriff auf personenbezogene Daten ermöglichen,

- die Verarbeitung von personenbezogenen Daten für rechtswidrige Zwecke ermöglichen oder
- die Sicherheit der Mitarbeiter und Mitarbeiterinnen gefährden.

Die Nichteinhaltung dieser Dienstanweisung kann zu einer der nachfolgenden Sanktionen führen, ist aber nicht auf diese beschränkt:

- disziplinarische oder arbeitsrechtliche Folgen,
- straf- und/oder zivilrechtliche Verfahren oder
- Haftung und Regressforderungen.

3 Datensicherheit

3.1 Allgemeines

Die Datensicherheit umfasst alle technischen und organisatorischen Maßnahmen im Sinne des § 10 DSG NRW für Daten und Objekte. Dabei sind Maßnahmen zu treffen, die sicherstellen, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit der Daten),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität der Daten),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit der Daten),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität der Daten),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit der Daten), und
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, so dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz der Verfahren).

Die Sachbereiche des Gemeindekassenverbandes Altenberge - GKV - haben die Sicherstellung der datenschutzrechtlich zulässigen Speicherung und Nutzung der Daten zu gewährleisten. Gespeicherte Daten (z.B. auf Disketten, Festplatten, CDs oder DVD´s, Magnetbändern, Mikrofichen) und Akten mit personenbezogenen Daten sind verschlossen und vor äußeren Einflüssen, insbesondere vor ungerechtfertigter Nutzung, geschützt aufzubewahren.

Die Regelungen dieses Abschnittes der Dienstanweisung gelten auch für nicht IT-gestützte Vorgänge (Bearbeitung von Karteien, Listen, Akten usw.).

3.2 Besondere Regelungen bei der IT-Nutzung

Die Sachbereiche sowie die für den IT-Bereich zuständige Stelle haben durch technische und organisatorische Maßnahmen sicherzustellen, dass informationstechnische Einrichtungen, Daten- und Programmbestände vor Verlust, Zerstörung, unsachgemäßer Behandlung, unbefugter Einsichtnahme u.a. geschützt sind.

Zu den Maßnahmen zählen insbesondere:

- die Erstellung von Zugriffskonzepten,
- die Festlegung von Zugangsberechtigungen,
- die Festlegung besonderer, fachbereichsspezifischer Regelungen über den Umgang mit personenbezogenen Daten,
- die Sicherung personenbezogener Daten (vgl. 3.4) und
- Passwörter (vgl. 3.2.3).

Personenbezogene Daten dürfen nur genutzt werden, wenn sie zulässig erhoben oder von Dritten rechtlich begründet übermittelt wurden. Bereichsspezifische Rechtsvorschriften sind zu beachten. Daten und Programme sind regelmäßig zu sichern.

Auftretende Störungen bzw. Unregelmäßigkeiten im Bereich der Datenverarbeitung sind den Administratoren des GKV unverzüglich mitzuteilen.

3.2.1 Zuständigkeit

Die Sicherstellung eines ordnungsgemäßen Betriebsablaufs aller Datenverarbeitungssysteme in (sicherheits-) technischer Hinsicht ist – in Abstimmung mit den Sachbereichen - Aufgabe des IT-Bereichs des GKV.

3.2.2 Zugriffsschutz

Der Zugriffsschutz umfasst Maßnahmen, die sicherstellen, dass nur Berechtigte auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Dies wird dadurch erreicht, dass

- der Sachbereich die Zugriffs- und Nutzungsberechtigungen jedes Mitarbeiters/jeder Mitarbeiterin festlegt und dem IT-Bereich des GKV mitteilt,
- der Zugriff auf Programme und gespeicherte Daten grundsätzlich nur durch Erteilung einer besonderen Berechtigung möglich ist,
- der berechtigte Zugriff grundsätzlich nur über Eingabe eines Passwortes durch den Benutzer möglich ist und
- die Nutzung von Anwendungen gegebenenfalls auf bestimmte Endgeräte beschränkt wird.

Veränderungen durch Umsetzungen bzw. geänderte Aufgabenzuweisungen der Nutzer/innen sind durch den Sachbereich dem GKV unverzüglich mitzuteilen.

3.2.3 Passwörter

Grundsätzlich sollen die Benutzer/innen in die Lage versetzt werden, ihre Passwörter selbst zu vergeben und zu ändern. Ist dies verfahrensbedingt nicht möglich, erfolgt die Verwaltung durch die Administratoren des GKV.

Die Benutzer/innen haben die Passwörter strikt geheim zu halten (auch gegenüber Vorgesetzten, Auszubildenden etc.). Bei unbeabsichtigtem Bekannt werden des Passwortes ist jeder Mitarbeiter verpflichtet, sich unverzüglich ein neues Passwort

zuteilen zu lassen oder das Passwort selbst zu ändern. Die Eingabe der Passwörter hat unbeobachtet zu erfolgen. Aufzeichnungen über Passwörter sind nicht zulässig. Die Passwörter sind in der Regel spätestens alle 90 Tage zu ändern. Bereits benutzte Passwörter dürfen nicht nochmals verwendet werden. Die Passwörter müssen aus mindestens sechs Zeichen, darunter Buchstaben und Ziffern bestehen.

3.2.4 Zugriff durch berechtigte Dritte

Ein Zugriff Dritter auf die installierte Hard- und Software darf nur im Rahmen einer schriftlichen Auftragsvergabe bzw. eines Wartungs- bzw. Fernwartungsvertrages erfolgen. Bei Remote-Zugriffen o. ä. ist eine ausdrückliche Erlaubnis im Einzelfall und nur für die Dauer des Zugriffs durch den GKV erforderlich. Dauer und Grund sind zu dokumentieren. Dabei ist sicherzustellen, dass Dritte nur personenbezogene Daten zur Kenntnis nehmen können, wenn dies im Rahmen der Aufgabenerfüllung unvermeidlich ist. Zugriffe vor Ort durch Dritte sind nur in Anwesenheit von Mitarbeiter/innen des GKV gestattet.

Die Regelungen zu 2.5 gelten entsprechend.

3.2.5 Datenträgeraustausch

Beim Versand von Datenträgern ist sicherzustellen, dass der Empfänger oder die Empfängerin nur die für ihn/sie bestimmten Daten erhält. Stellen, die Datenträgeraustausch durchführen, müssen einen Datenträgernachweis führen. Zu- und Abgänge sind mit Angabe der übergebenden bzw. übernehmenden Person, zum Datenträgerinhalt und zum Anlass des Transports zu vermerken.

Der Versand oder Transport von Datenträgern mit personenbezogenen Daten muss in der Weise geschehen, dass eine Beschädigung der Datenträger oder ein unberechtigter Zugriff auf die Daten möglichst ausgeschlossen werden kann (z.B. im luftgepolsterten, versiegelten Umschlag oder im speziellen abgeschlossenen Transportbehältnis). Dem Datenträger ist ein Begleitschein beizufügen, auf dem der Eingang vom Empfänger zu bestätigen ist.

3.3 Zugangsschutz

Die Regelung des Zugangs und der Aufbewahrung personenbezogener Daten richtet sich nach deren Sensibilität und obliegt den Sachbereichen. Der Zugangsschutz umfasst Maßnahmen, die sicherstellen, dass Unbefugten der Zugang zu Datenverarbeitungsanlagen und sonstigen Unterlagen mit personenbezogenen Daten verwehrt wird.

3.3.1 Räume

Räume, in denen personenbezogene Daten elektronisch oder in Akten vorhanden sind, sind bei Abwesenheit der Mitarbeiter/innen zu verschließen.

Der Zutritt zu den Räumen, in dem zentrale Netzwerk- und Serverkomponenten untergebracht sind, ist nur den speziell hierzu bevollmächtigten Mitarbeiter/innen erlaubt.

3.3.2 Endgeräte

Die Inbetriebnahme der Rechner ist nur mittels eines Passwortes möglich. Räume, in denen sich Rechner (z. B. PCs) befinden, sind bei Abwesenheit der Mitarbeiter/innen zu verschließen. Auch bei kurzer Abwesenheit sind Programme und Anwendungen soweit zu sperren, dass ein erneutes Arbeiten erst nach erneuter Eingabe eines Passwortes möglich ist, sofern ein anderer technischer Zugriffsschutz nicht besteht. Die Standorte der Rechner und Zusatzgeräte (z. B. Drucker) dürfen ohne vorherige Absprache mit dem GKV nicht verändert werden.

3.4 Datensicherung

Die Datensicherung umfasst alle technischen Maßnahmen, die sicherstellen, dass die verarbeiteten Daten vor Verlust durch technische Defekte, Fehlbedienung und vor Verlust durch Datenmissbrauch geschützt werden. Grundsätzlich hat die Speicherung aller Daten auf den zentralen Servern zu erfolgen.

Einzelheiten der Datensicherung sind in einem Datensicherungskonzept, das der GKV in Abstimmung mit den Fachbereichen erstellt, festzulegen. Durchgeführte Sicherungen sind zu protokollieren, die Datenträger sind an besonderer Stelle aufzubewahren.

3.5 Überlassung von Zubehör

Die durch den GKV zur Verfügung gestellten Datenträger, Software- und Hardwarekomponenten sowie Systemliteratur sind in geeigneter Weise unter Verschluss zu halten. Eine Verwendung außerhalb der Dienstgebäude ist nur in Abstimmung mit dem GKV zulässig.

3.6 Einsatz und Verwendung von Programmen und Verfahren

3.6.1 Hardware

Änderungen der Hardware-Konfiguration, insbesondere der Einbau von Komponenten, Anschluss von Druckern oder anderer externer Zusatzgeräte sind ausschließlich dem GKV vorbehalten.

Die Verwendung privater Hardware bzw. Datenträger ist untersagt. Über Ausnahmen hiervon entscheidet der GKV.

3.6.2 Software

Neue Verfahren bzw. wesentlich geänderte Verfahren dürfen erst eingesetzt werden, wenn die Freigabe aus dem Fachbereich schriftlich vorliegt und die Vorabkontrolle im Sinne des § 10 Abs. 3 DSG NRW erfolgt ist (vgl. 2.3.3.3). Bei Vorliegen wichtiger Gründe können Verfahren vorläufig freigegeben werden.

Sollen auf Basis von Standard-Software Anwendungen selbst entwickelt werden, ist wie folgt vorzugehen:

- Mit der Entwicklung darf erst begonnen werden, wenn der Fachbereich, der/die DSB und der GKV diesem Vorhaben zugestimmt haben.
- Für alle selbst entwickelten Anwendungen gelten die Regelungen dieser Dienstanweisung für Verfahren entsprechend.
- Von diesen Bestimmungen ausgenommen sind Anwendungen, die offenkundig nur der Lösung von Einzelfällen dienen und nicht zum wiederholten Gebrauch bestimmt sind (z.B. Berechnungen mit Hilfe einer Excel-Tabelle). Die datenschutzrechtlichen Bestimmungen zur Verarbeitung personenbezogener Daten bleiben unberührt.

Die Konfiguration der Arbeitsplatzrechner erfolgt durch den IT-Bereich des GKV. Zum Nachweis bestehender Softwarelizenzen verbleiben die Originaldatenträger nach dem Aufspielen beim IT-Bereich des GKV.

Es ist grundsätzlich untersagt,

- Änderungen in der bestehenden Konfiguration, insbesondere das Aufspielen zusätzlicher Dateien und Programme, vorzunehmen,
- private Software oder Daten zu verwenden oder
- Programme weiterzugeben oder zu verändern.

Über Ausnahmen entscheidet der GKV.

3.7 Mobile Endgeräte

Der Einsatz mobiler Endgeräte (Notebooks, Laptops, Personal Digital Assistants – PDAs -, Smart Phones etc.) erfordert wegen der erhöhten Gefahr des unberechtigten Zugriffs durch Dritte und/oder Diebstahls besonderer Vorsichtsmaßnahmen.

3.7.1 Authentisierung und Verschlüsselung

Bei mobilen PCs etc. muss das BIOS-Bootpasswort aktiviert werden, wenn dessen Nutzung möglich ist. Erst nach Eingabe des korrekten Bootpasswortes kann der Computer gestartet werden. Falls vorhanden, müssen ähnliche Verfahren bei anderen mobilen Endgeräten ebenfalls aktiviert sein. Der GKV verfügt ebenfalls über das Passwort, ggf. das Administratoren-Passwort zum Aufheben von BIOS-Benutzerpasswörtern.

Ist keine Passwortnutzung auf BIOS-Ebene möglich, müssen die Daten auf dem mobilen Endgerät verschlüsselt werden. Ist eine Verschlüsselung nicht möglich, dürfen schutzbedürftige Daten nicht auf dem mobilen Endgerät gespeichert werden. Stattdessen sind Wechselmedien (USB-Sticks, CDs, Disketten) als Datenträger zu verwenden, die getrennt vom mobilen Endgerät aufzubewahren bzw. zu transportieren sind.

3.7.2 Handys, Smart Phones etc.

Beim Einsatz von Handys, insbesondere jedoch von Smart Phones mit schutzbedürftigen Daten, darf die PIN-Abfrage zur Nutzung des mobilen Endgerätes und auch die PINB zur Nutzung der Mailbox nicht deaktiviert werden. Herstellerseitig

voreingestellte PINs sind unverzüglich abzuändern und der Amtsleitung mitzuteilen.

3.8 Verfahrensverzeichnis

Für jedes Verfahren, in dem personenbezogene Daten automatisiert verarbeitet werden, haben die Sachbereiche eine Verfahrensbeschreibung zu erstellen und dem/der DSB vorzulegen. Das Verfahrensverzeichnis ist von dem/der DSB zu führen.

3.9 Vorabkontrolle

Unter „Vorabkontrolle“ ist eine Untersuchung zu verstehen, ob durch die automatisierte Datenverarbeitung das Grundrecht der informationellen Selbstbestimmung möglicherweise gefährdet wird. Vor dem Einsatz oder der wesentlichen Änderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten ist sie von dem/der DSB durchzuführen. Die Fachbereiche haben hierfür die erforderlichen Angaben zu machen.

3.10 Entsorgung von Datenträgern

Auf maschinell einsetzbaren Datenträgern (beispielsweise Disketten, Festplatten, CDs, DVDs, Speicherkarten etc.), die an Herstellerfirmen zurückgehen, verkauft werden sollen oder nicht mehr verwendbar sind, sind noch vorhandene personenbezogene oder vertrauliche Daten physikalisch zu löschen.

Hinweis: Das einfache Löschen und/oder Formatieren der Datenträger reicht nicht aus! Falls eine physikalische Löschung nicht möglich sein sollte, sind die Datenträger in geeigneter Weise für die Verarbeitung unbrauchbar zu machen.

Ist die Löschung der Daten technisch nur durch Dritte möglich, ist eine Weitergabe der Datenträger an diese zulässig, wenn der sichere Transport gewährleistet, eine missbräuchliche Nutzung der Daten ausgeschlossen und ihre unverzügliche vollständige Löschung garantiert wird. Dies ist durch eine schriftliche Vereinbarung mit den Dritten zu gewährleisten.

Werden Daten von Dritten gelöscht oder Datenträger vernichtet, sind die Musterrahmenverträge zur Auftragsdatenverarbeitung gem. § 11 DSG NRW i. V. m. § 80 SGB X zu beachten. Die Regelungen zu 2.5 gelten entsprechend.

Im Übrigen gelten die Regelungen zu 3.2.5.

Entsprechendes gilt für Daten in nichtelektronischer Form wie Akten, Niederschriften pp., wobei das Archivgesetz und sonstige gesetzliche Aufbewahrungsfristen zu beachten sind.

4 Schlussbestimmungen

Diese Dienstanweisung tritt mit Ihrer Unterzeichnung in Kraft. Gleichzeitig wird die Dienstanweisung für den Einsatz und die Nutzung der Informations- und Kommunikationstechnik des Gemeindekassenverbandes Altenberge vom 26.1.1988 außer Kraft gesetzt.

Altenberge, den 1.8. .2007

gez. Paus

Verbandsvorsteher