Rheinische Versorgungskassen

Beauftragter für Datenschutz, Informationsfreiheit und IT-Sicherheit

Jahresbericht 2017

Version: 1.1

Stand: 05.07.2018

Autor: Dirk Erdmann,
Beauftragter für Datenschutz, Informationsfreiheit und IT-Sicherheit

Status: abgenommen

Rheinische Versorgungskassen
Mindener Straße 2, 50679 Köln, Tel. 0221 8273-0
www.versorgungskassen.de, info@versorgungskassen.de

Versionshistorie

Version	Datum	Name	Änderung
1.0	19.02.2018	Dirk Erdmann	Ersterstellung
1.0	01.03.2018	Dirk Erdmann	Anpassungen und Korrekturen
1.0	19.04.2018	Dirk Erdmann	Anpassungen und Korrekturen
1.0	14.06.2018	Dirk Erdmann	Anpassungen und Korrekturen
1.0	05.07.2018	Dirk Erdmann	Anpassungen und Korrekturen

Abnahmehistorie

Version	Datum	Name der Teilnehmer bei Doku-Review	Hinweise / Datum Doku-Review
1.1	10.07.2018	Miguel Freund	Abnahme durch Geschäftsführer

Inhaltsverzeichnis

1 Einführung

1.1 Grundlagen

Die Rheinischen Versorgungskassen (RVK) sind errichtet durch § 1 (1) des Gesetzes über die kommunalen Versorgungs- und Zusatzversorgungskassen im Lande Nordrhein-Westfalen vom 06.11.1984 (VKZVKG). Sie sind eine Körperschaft des öffentlichen Rechts und unterstehen der Rechtsaufsicht, die Zusatzversorgungskasse zusätzlich der Versicherungsaufsicht des Ministeriums für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen. Nach § 1 (2) VKZVKG und § 5 (1) c) Nr. 3 LVerbO obliegt die Geschäftsführung der Rheinischen Versorgungskassen dem Landschaftsverband Rheinland (LVR).

Die Rheinischen Versorgungskassen gliedern sich in die Versorgungskasse und Zusatzversorgungskasse. Die Aufgaben für die Mitglieder der Versorgungskasse sind die Berechnung und Zahlung von beamtenrechtlichen Versorgungsleistungen, für die Mitglieder der Beihilfekasse Berechnung und Zahlung von Beihilfen an Versorgungsempfänger und aktive Beamte und Beschäftigte. In der Zusatzversorgungskasse umfassen die Aufgaben nach Maßgabe tarifvertraglicher Regelungen die Gewährung einer die gesetzliche Rente ergänzenden, zusätzlichen betrieblichen Alters-, Erwerbsminderungs- und Hinterbliebenenversorgung durch Versicherung. Darüber hinaus werden von den Rheinischen Versorgungskassen auch Personalentgeltberechnung und Zahlung sowie als Landesfamilienkasse Kindergeldleistungen für Mitglieder erbracht. Abschließend bieten die RVK auch die treuhänderische Verwaltung von Versorgungsrücklagen zur Rückdeckung zukünftiger Pensionsverpflichtungen ihrer Mitglieder an.

Das Geschäftsgebiet der Rheinischen Versorgungskassen umfasst die Regierungsbezirke Düsseldorf und Köln im rheinischen Teil des Landes Nordrhein-Westfalen und das Gebiet der ehemaligen Regierungsbezirke Koblenz und Trier in Rheinland-Pfalz (nach dem Stand vom 30.09.1968 - ehemalige Rheinprovinz).

Pflichtmitglieder der Versorgungskassen (VK) sind die kreisangehörigen Gemeinden ohne die Städte. Andere Gemeinden und Gemeindeverbände und sonstige Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, Fraktionen des Landtags sowie kommunale Spitzenverbände und vergleichbare kommunale Spitzenorganisationen mit Sitz im Geschäftsgebiet und juristische Personen des privaten Rechts mit überwiegend kommunaler Beteiligung oder kommunalen Aufgaben können als freiwillige Mitglieder zugelassen werden.

Mitglieder der Zusatzversorgungskasse (ZVK) können die Gemeinden und Gemeindeverbände im Geschäftsgebiet, andere juristische Personen des öffentlichen Rechts, kommunale Spitzenverbände und vergleichbare kommunale Spitzenorganisationen, Verbände von Körperschaften des öffentlichen Rechts, die Fraktionen des Deutschen Bundestags, des Landtags und kommunaler Vertretungen sowie juristische Personen des privaten Rechts mit überwiegend kommunaler Beteiligung, kommunalen Aufgaben oder kommunaler Risikoabdeckung sein.

1.2 Der Beauftragte für Datenschutz, Informationsfreiheit und IT-Sicherheit

Gemäß § 32a (1) des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) sind die Rheinischen Versorgungskassen verpflichtet, einen behördlichen Datenschutzbeauftragten zu bestellen. Die RVK unterstehen durch die Regelungen des Landesdatenschutzrechts der Fachaufsicht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen in Düsseldorf.

Der Geschäftsführer der Rheinischen Versorgungskassen hat mit Wirkung zum 22.05.2001 Herrn Dirk Erdmann zum Datenschutzbeauftragten bestellt. Zum 8. Januar 2010 wurde die Bestellung zum Beauftragten für Datenschutz, Informationsfreiheit und IT-Sicherheit (BDII) der Rheinischen Versorgungskassen ausgeweitet. Gleichzeitig ist der Beauftragte der RVK seit 01.07.2003 als externer Datenschutzbeauftragter nach § 7a (2) BbgDSG in gleicher Funktion zum Beauftragten für Datenschutz, Informationsfreiheit und IT-Sicherheit des Kommunalen Versorgungsverbands Brandenburg (KVBbg) in Gransee bestellt, mit dem nach der ursprünglichen Errichtungsbeauftragung durch die RVK eine Vereinbarung zur Kooperation auf dem Gebiet der Informationstechnologie besteht.

Das Tätigkeitsfeld des Beauftragten für Datenschutz, Informationsfreiheit und IT-Sicherheit umfasst für den Bereich Datenschutz die Wahrnehmung aller Aufgaben des Datenschutzbeauftragten nach dem DSG NRW sowie nach dem Bundesdatenschutzgesetz (BDSG), soweit zutreffend. Insbesondere gehört dazu die Sicherstellung der Einhaltung der datenschutzrechtlichen Vorgaben im operativen Geschäft und der IT-Unterstützung der einzelnen Geschäftsbereiche der RVK.

Die erforderliche Fachkunde wird durch regelmäßigen Besuch von Fortbildungs- und Kongressveranstaltungen erhalten und ausgebaut. Weiterhin arbeitet der BDII im Arbeitskreis „Entwicklung des Datenschutzrechts“ der vom Bundeswirtschaftsministerium geförderten Arbeitsgemeinschaft für wirtschaftliche Verwaltung eV (AWV) in Eschborn mit. Dieser Arbeitskreis fungiert als einer der nationalen Interessenverbände gegenüber dem Gesetzgeber auf nationaler und europäischer Ebene. Die Rheinischen Versorgungskassen sind bei der AWV Mitglied.

Zwischenzeitlich wurde außerdem der Vorsitz des Forums Datenschutz bei der Dachorganisation AKA (Arbeitsgemeinschaft kommunale und kirchliche Altersversorgung) e.V. in München übernommen.

Im Bereich Informationsfreiheit gehört die federführende Bearbeitung aller Vorgänge nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) zum Tätigkeitsspektrum des BDII, hier allem voran die Entscheidung über eine bestehende Offenlegungspflicht evtl. angeforderter Unterlagen und Vorgänge.

Die Gewährleistung der IT-Sicherheit bildet den dritten Aufgabenbereich des BDII. Hierzu gehören alle Tätigkeiten zur Regelung in eigener Zuständigkeit der Kassen und in Abstimmung mit dem Sicherheitsbeauftragten des Produktionsrechenzentrums InfoKom des Landschaftsverbandes Rheinland (LVR). Hier ist der Datenschutzbeauftragte der RVK geborenes Mitglied im Beirat für IT-Sicherheit von LVR-InfoKom und nimmt dadurch auch Einfluss auf die Sicherheitsstandards des IT-Betriebs insgesamt. Dazu gehört beispielsweise das periodisch fortgeschriebene umfangreiche Datenschutzhandbuch im Sinne eines Datenschutz-Managementsystems.

1.3 Datenschutzbericht 2017

Eine Verpflichtung der RVK zu einem periodischen Bericht über die Aufgabenerledigung des BDII besteht mit Blick auf die Regelungen des DSG NRW derzeit nicht. Um den steigenden Anforderungen aus den Bereichen Compliance und Risikomanagement des eigenen Hauses sowie aus den Reihen der Mitglieder jedoch entgegenzukommen, wird auch für 2017 ein ausführlicher und umfassender Tätigkeitsbericht vorgelegt bzw. fortgeschrieben. Der Bericht betrifft den Zeitraum 1. Januar bis 31. Dezember 2017 und erstreckt sich auf die drei Aufgabenbereiche Datenschutz, Informationsfreiheit und IT-Sicherheit.

2 Datenschutz

2.1 Entwicklung des Datenschutzrechts 2017

Internationales Recht und Recht der Europäischen Union

Das Jahr 2017 stand ganz im Zeichen der Diskussion und Vorbereitung des Wirksamwerdens der DS-GVO. Die Aufsichtsbehörden haben verschiedene Umsetzungshilfen zu einzelnen Artikeln und Fragestellungen der DS-GVO veröffentlicht. Gleichwohl schien es auch hier noch unterschiedliche Auffassungen zu geben. Gleiches gilt für die Verbände und Organisationen wie die GDD (Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn) oder den BvD (Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Berlin), auch hier wurden Dokumente, Mustertexte und andere Unterlagen erstellt, um die Einführungsphase des europäischen Rechts zu begleiten.

Im November 2017 wurde eine erste Korrektur der DS-GVO durch die EU vorgenommen, um verschiedene redaktionelle Fehler in einzelnen Sprachfassungen zu korrigieren. Hierbei ist allerdings keine die RVK betreffende Regelung berührt.

Weiterhin als sehr kritisch ist die Grundlage des Datentransfers zwischen Europäischer Union und den USA zu sehen. Der Privacy Shield als Nachfolger des gekippten Save Harbour-Abkommens unterliegt einigen Kritikpunkten der europäischen Datenschutzaufsichten, so dass nicht unbedingt mit seinem Fortbestand zu rechnen ist. Erforderlicher Datenaustausch mit den USA muss dann mit den verbleibenden Mitteln der DS-GVO geregelt werden, bis es ein neues beiderseitiges und dauerhaftes generelles Abkommen gibt.

Bundesrecht

Im Sommer 2017 ist es der alten Bundesregierung noch gelungen, zum Ende der Legislatur das DS-GVO-Anpassungsgesetzes als Artikelgesetz zu verabschieden. Kerninhalt ist das neue Bundesdatenschutzgesetz vom 30.06.2017, das gleichfalls am 25.05.2018 in Kraft tritt. Gleichzeitig ist es das erforderliche Umsetzungsgesetz für die EU-Datenschutzrichtlinie Polizei und Justiz. Das BDSG gilt weiterhin für den öffentlichen Bereich des Bundes und den gesamten nichtöffentlichen Bereich, außerdem für den öffentlichen Bereich der Länder, wenn er in seiner Aufgabenerfüllung im Wettbewerb steht oder privatrechtlich auftritt.

Zur Anpassung des Bereichsrechts des Bundes ist ein weiteres DS-GVO-Anpassungsgesetz geplant, das gleichfalls als Artikelgesetz die entsprechenden Bundesgesetze an die zukünftigen Regularien anpassen soll. Im Berichtszeitraum ist dieses noch nicht verabschiedet worden.

Weitere im Kontext neuen europäischen Rechts in Kraft getretene Gesetze haben für den Aufgabenvollzug der RVK keinen Belang.

Landesrecht Nordrhein-Westfalen

Ähnliches gilt nach wie vor für den Landesgesetzgeber Nordrhein-Westfalen. Auch hier hat es im Berichtszeitraum am Vorabend der europäischen und nationalen Neuordnung des Datenschutzrechts keinerlei Gesetzesinitiativen mehr gegeben, so dass das für die Versorgungskassen primär geltende Landesdatenschutzgesetz weiterhin unverändert in 2017 galt.

Vorbereitende Initiativen mit Blick auf die kommende Grundverordnung sind ebenfalls nicht bekannt geworden.

Telekommunikationsrecht

Auch im Telekommunikationsrecht gab es im Berichtszeitraum wiederum keine Anhaltspunkte für gravierende Rechtsänderungen. Die geplante ePrivacy-Verordnung der EU wurde nicht beschlossen, die Diskussion um diese dritte Säule der europäischen Datenschutzrechts-Reform hält noch an, eine weitere Terminplanung zur Verabschiedung liegt noch nicht vor.

2.2 Tätigkeitsbericht 2017

Die Arbeit des BDII umfasst im laufenden Geschäft die Sicherstellung des Datenschutzes. Dies geschieht durch Mitwirkung bei allen entsprechenden Verwaltungsvorgängen, Zustimmung zu personellen Entscheidungen im Rahmen der Telearbeit, Beratung des Personalrates, Beratung der Mitarbeiter bei relevanten Fragestellungen, Bearbeitung eingegangener Petitionen an die Datenschutzaufsichtsbehörde LDI NRW und Initiativen durch aktuelle Ereignisse oder Weiterentwicklung der Systeme durch funktionalen und/oder technischen Fortschritt.

Im Einzelnen waren Inhalte (verkürzte Sachverhalte) unter anderem:

2.2.1 Verfahren mit der Aufsichtsbehörde LDI Nordrhein-Westfalen

Im Berichtszeitraum wurde das Verfahren mit der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW zur Frage der Zulässigkeit der Telearbeit bei der Verarbeitung hochsensibler Daten im Kontext des Beschäftigtendatenschutzes weitergeführt. Ein Abschluss des Verfahrens konnte in 2017 nicht mehr erreicht werden.

2.2.2 Unmittelbare Beschwerden oder Eingaben an die RVK

Im Berichtszeitraum hat es keine unmittelbaren Beschwerden oder sonstige Anfragen an den Beauftragten für Datenschutz der RVK gegeben.

2.2.3 Berechtigungswesen

Fortlaufende Anpassung der funktionsbezogenen Berechtigungsrollen sowie einzelner Rechte an die tatsächlichen Erfordernisse vor allem zur Nutzung der SAP-Module. Hier ist eine dauerhafte Aufgabe mit Blick auf laufende Be- und Entrechtigungen einzelner Mitarbeitenden oder Gruppen zu sehen.

2.2.4 Datenschutz-Konzept SAP-System RVK

Für das bestehende SAP-System der RVK im Verbund der SAP-Welt von LVR-InfoKom ist ein datenschutzrechtliches Betriebskonzept weiterhin im Aufbau, um Transporte, Testszenarien, Mandantenkopien, Migrationen usw. einheitlich und verbindlich zu regeln. Besonderes Gewicht liegt dabei auf die Verwendung von Test- und pseudonymisierten Anwenderdaten auf den unterschiedlichen Systemumgebungen.

Dabei gilt es Handlungsbedarf zu erkennen und Maßnahmen zu ergreifen, die nicht durch das vorhandene Datenschutz-Managementsystem gedeckt sind.

2.2.5 Beschäftigten-Datenschutz

Beteiligung an allen Genehmigungsverfahren zur Gewährung von Heim-/Telearbeit für die Mitarbeitenden der Rheinischen Versorgungskassen.

2.2.6 Intra-/Internetauftritt der RVK

Fortlaufende Beratung der zuständigen Fachabteilung bei der Neugestaltung des Intra- und Internetauftritts in datenschutzrechtlicher Sicht.

2.2.7 Schulungen

Durchführung von bedarfsorientierten Schulungen und Unterweisungen für Mitarbeitende der RVK und ihrer Mandanten, Beiträge in der unregelmäßig erscheinenden Mitarbeiterzeitschrift WiRVK. Schwerpunkte liegen nach wie vor auf einer weiteren Sensibilisierung und Schaffung einer dauerhaften Awareness für Datenschutz und Datensicherheit.

2.2.8 Überregionale Aktivitäten

AKA-Forum Datenschutz

Ein weiteres Treffen des Forums Datenschutz der AKA fand im Herbst 2016 statt, um gemeinsame Vorgehensweisen und Umsetzungsaktivitäten mit Blick auf die DS-GVO und das kommende neuen nationale Recht für 2017 zu planen und abzustimmen. Ein initiales Treffen eines zusätzlichen AKA-Forums „IT-Sicherheit“ hat gleichfalls im Berichtszeitraum stattgefunden. Auch bei diesem Thema sollen Erfahrungen zwischen den Versorgungseinrichtungen ausgetauscht werden, um Synergien zu gewinnen.

AWV-Arbeitskreis „Entwicklung des Datenschutzrechts“

Teilnahme an den Sitzungen des Arbeitskreises, aktuell mit Themen der Umsetzung des neuen europäischen und nationalen Rechts befasst.

2.2.9 Auftragsdatenverarbeitung

Im Berichtsjahr wurde die periodische Vorort-Überprüfung der Auftragnehmer der RVK, die Hilfs- und Unterstützungsarbeiten auf Basis einer Auftragsdatenverarbeitung vornehmen, weiterhin durchgeführt.

2.2.10 Prüfung durch Mitglieder

Im Berichtszeitraum wurden keine Vorort-Prüfungen durch Mitglieder der RVK durchgeführt.

2.3 Ausblick 2018

Das Jahr 2018 wird ganz im Zeichen der europäischen Datenschutz-Grundverordnung stehen, sie wird bekanntlich am 25.05.2018 wirksam werden. Parallel wird das neue Bundesdatenschutzgesetz in Kraft treten, ein neues Datenschutzgesetz NRW ist zum Ende des Berichtsjahres noch nicht in Sicht, wird aber vermutlich noch rechtzeitig verabschiedet werden. Zu beobachten ist flankierend inwieweit das jeweilige fachliche Bereichsrecht angepasst wird, das unverändert den Regelungen der Datenschutzgesetze vorgeht.

Mit Blick auf den Mai 2018 sind entsprechende Vorarbeiten zu leisten, um zum Stichtag eine weitgehende Rechtskonformität der Datenverarbeitung hinsichtlich des Schutzes personenbezogener Daten zu erzielen. Hierzu sind im Frühjahr noch weitere Abstimmungen auf Basis der Arbeitsgemeinschaft der Versorgungseinrichtungen geplant, um die notwendigen Arbeiten gemeinsam und synergetisch anzugehen.

Die Beratungs- und Schulungsaktivitäten sollen im neuen Jahr weiter fortgeführt werden, um das erreichte hohe Niveau zu erhalten und weiter auszubauen.

3 Informationsfreiheit

3.1 Entwicklung der Informationsfreiheits-Rechts 2017

Das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) vom 27. November 2001 ist seit dem 01.01.2002 gültig und seit dem 15.10.2014 keinen inhaltlichen Anpassungen unterlegen. Dieses Gesetz gewährt den Bürgerinnen und Bürgern in Nordrhein-Westfalen einen grundsätzlich freien Zugang zu allen bei den öffentlichen Stellen des Landes vorhandenen Informationen. Darüber hinaus gibt es, ähnlich wie in anderen Bundesländern, in Nordrhein-Westfalen noch ein spezielles Umweltinformationsgesetz (UIG NRW) sowie neben dem Gesetz zur Regelung des Zugangs zu Informationen des Bundes (IFG) das Verbraucherinformationsgesetz (VIG) für spezielle Rechtsbereiche.

3.2 Tätigkeitsbericht 2017

Im Herbst 2017 ist es zu einem Verfahren nach § 4 IFG NRW gekommen, durch das Auskünfte in Bezug auf Abrechnungsmodalitäten anlässlich des Ausscheidens eines Mitglieds der Zusatzversorgung beantragt wurden. Der Antrag auf Informationszugang war jedoch bereits aus formalen Gründen abzulehnen.

Weitere Verfahren haben sich nicht ergeben.

3.3 Ausblick 2018

In 2018 wird das IFG NRW durch die erforderliche Anpassung des Landesrechts NRW an das zu erwartende neue Datenschutzgesetz zu ändern sein, um den Anforderungen des EU-Rechts zu genügen.

Weiterhin ist die Rechtsprechung zu beobachten, um bei eventuellen weiteren Verfahren nach dem IFG NRW für die RVK rechtskonform handeln zu können. Insbesondere sind auch die Handlungshinweise des LDI NRW zu beachten, die schnell Grundlage und Maßstab vorprozessualer und prozessualer Verfahren und Entscheidungen sind.

4 IT-Sicherheit

4.1 Grundlagen

Die Rheinischen Versorgungskassen haben derzeit keinen eigenen operativen IT-Betrieb. Aufgrund der gesetzlich geregelten Geschäftsführung durch den Landschaftsverband Rheinland wird das Rechenzentrum LVR-InfoKom als IT-Dienstleister des Landschaftsverbandes Rheinland genutzt. Gleichwohl handelt es sich bei den eingesetzten IT-Verbundlösungen für Geschäftsbereiche der Versorgungskassen um kasseneigene Systeme.

Für die IT-Strukturen bedeutet dies, dass alle operativen Systeme ihren Standort in den beiden Rechenzentren in Köln haben und die RVK dorthin mit mehreren redundanten und unabhängigen sicheren Breitbandverbindungen angeschlossen sind. Anwendungen und Daten aller betroffenen Systeme sind daher auf Servern und Systemen bei LVR-InfoKom in Betrieb bzw. gespeichert und obliegen den dort gültigen Sicherheitsbestimmungen, die periodisch durch Wirtschaftsprüfer und Rechnungsprüfungseinrichtungen geprüft und kontrolliert werden. Der Einsatz der Anwendungen inkl. des Zugriffs auf alle Daten erfolgt über ein Terminalserversystem, um neben praktischen vor allem alle erforderlichen Sicherheitsaspekte besonders gut berücksichtigen zu können. Personenbezogene Daten können nur in dieser Umgebung verarbeitet werden, so dass keine derartigen Daten auf Clients gleich welcher Art gelangen. Alle mobilen Geräte werden unverändert durch ein Mobile-Device-Management-System (MDM) geschützt.

4.2 IT-Sicherheitslage und -maßnahmen 2017

Verantwortlich aus Sicht der RVK für den sicheren RZ-Betrieb ist LVR-InfoKom. Anforderungen an die Sicherheit werden von den RVK und ihren Mandanten als gemeinsamer Betreiber entsprechender Fachanwendungen und unter Berücksichtigung aller Anforderungen aus dem Risikomanagement formuliert und zur Umsetzung und Berücksichtigung beauftragt.

Um den Anforderungen nicht zuletzt auch eigener LVR-interner Kunden zu genügen, ist der RZ-Betrieb von LVR-InfoKom derzeit regelmäßig nach ISO 27001 zertifiziert. Außerdem wird jährlich eine Prüfung durch einen unabhängigen Wirtschaftsprüfer nach IDW PS 951 durchgeführt und entsprechend bestätigt, neben den regelmäßigen Prüfungen durch den LVR-eigenen Fachbereich Rechnungsprüfung.

Im Rahmen der Prüfungen der RVK untersucht auch hier der jeweils beauftragte Wirtschaftsprüfer im Rahmen der Jahresprüfung alle Maßnahmen in Zusammenhang mit dem Risikomanagement. Der IT-Bereich ist hier nicht ausgenommen und steht insbesondere im Fokus eigenständiger Prüfungstätigkeiten.

LVR-InfoKom führt darüber hinaus regelmäßig interne und externe Audits inkl. entsprechender Penetrationstests in wichtigen, sicherheitsrelevanten Bereichen durch. Evtl. dabei festgestellte Unzulänglichkeiten werden jeweils schnellstmöglich abgestellt.

Damit sind nach wie vor grundlegend alle erforderlichen Rahmenbedingungen für einen sicheren IT-Betrieb geschaffen als Grundlage aller technisch-organisatorischen Maßnahmen im Sinne des Datenschutzrechts. Zahlreiche Dienstvereinbarungen und Dienstanweisungen regeln in Auskleidung der IT-Sicherheitsrichtlinien und der gültigen Sicherheitspolicy Details für Anwender und Anwendungen, um Awareness zu schaffen und die Einhaltung der Vorgaben zu gewährleisten. Die Einhaltung ist ebenfalls Inhalt automatisierter Prüfungen mit entsprechenden Maßnahmen.

Nach Verabschiedung des IT-Sicherheitsgesetzes des Bundes (ITSG/Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) am 17.07.2015 wurde die erforderliche Verordnung zu den kritischen Infrastrukturen, für die eine ganze Reihe von Auflagen gelten, am 02.05.2016 in einem ersten Teil erlassen. Der zweite Teil folgte durch Veränderungs-Verordnung vom 21.06.2017 mit Wirkung zum 30.06.2017. Dies umfasst nun neben Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung zusätzlich Gesundheit, Finanzen und Versicherungen sowie Transport und Verkehr. Unverändert ergibt sich keine unmittelbare Auswirkung auf die RVK oder einzelne Geschäftsbereiche.

4.3 Sicherheitsvorfälle 2017

Die bislang in den vergangenen Jahren ergriffenen Maßnahmen, Systemhärtungen und Sensibilisierungsmaßnahmen zeigen nach wie vor Erfolg und werden ständig weiterentwickelt, so dass Schadsoftware bislang immer rechtzeitig erkannt werden konnte oder sensible Systeme – dazu gehören alle produktiven Systeme – nicht unmittelbar angreifbar waren. Dadurch ergibt sich ein ganzheitliches und durchgängiges Schutzniveau des operativen IT-Betriebs der RVK, so dass es auch in 2017 zu keinen Sicherheitsvorfällen für die Versorgungskassen gekommen ist.

4.4 Ausblick 2018

Auch für das Jahr 20188 ist die Fortführung aller bisherigen Maßnahmen beabsichtigt und geplant, um eine weitere Absicherung des IT-Geschäfts gegen Angriffe von Innen und Außen zu erreichen. Die Awareness auf Anwenderseite soll auch zukünftig gestärkt werden, um eines der größten Betriebsrisiken zu minimieren.

Im Fokus bleibt daher auch die fortlaufende Überarbeitung der Notfallmaßnahmen, um bei gravierenden Störungen des IT-Betriebs die vorhandenen Risiken beherrschen und Schäden vermeiden zu können. Damit werden insbesondere Anforderungen aus dem Risikomanagement erfüllt. Das Thema ist aufgrund der Verflechtungen zwischen den Rheinischen Versorgungskassen, ihren Mandanten und LVR-InfoKom weiterhin übergreifend zu bearbeiten.

Außerdem sind weitere Abstimmungen im Rahmen des AKA-Forums IT-Sicherheit beabsichtigt, um Synergien und Erfahrungen aus den übrigen Versorgungseinrichtungen nutzen zu können.

5 Feststellung 2017

Dieser Jahresbericht wurde nach bestem Wissen und Gewissen erstellt. Er basiert auf den Angaben der Beteiligten oder auf selbst gewonnenen Erkenntnissen und gibt damit einen wesentlichen Einblick in die Aktivitäten des Berichtsjahres – ohne jedoch den Anspruch auf abschließende Vollständigkeit zu erheben.

Insgesamt sind ein datenschutzrechtskonformer Aufgabenvollzug zu attestieren, ebenso die grundsätzliche Einhaltung des Informationsfreiheits-Gesetzes NRW sowie ausreichend hoch ergriffene Sicherheitsmaßnahmen, um interne und externe Angriffe auf Systeme der RVK weitestgehend auszuschließen.

Zu meldepflichtigen Vorfällen nach Bundes- oder Landesdatenschutzrecht im Rahmen der für die Mitglieder der Rheinischen Versorgungskassen übernommenen Aufgaben ist es im Berichtszeitraum erneut nicht gekommen.

Köln, 10.07.2018

Dirk Erdmann

Beauftragter für Datenschutz,
Informationsfreiheit und IT-Sicherheit
der Rheinischen Versorgungskassen

1/2

6 Glossar

Begriff	Erklärung
AKA	AKA (Arbeitsgemeinschaft kommunale und kirchliche Altersversorgung) e.V., München (www.aka.de)
AWV	Arbeitsgemeinschaft Wirtschaftliche Verwaltung eV, Eschborn
BbgDSG	Brandenburgisches Datenschutzgesetz
BDII	Beauftragter für Datenschutz, Informationsfreiheit und IT-Sicherheit
BDSG	Bundesdatenschutzgesetz
BK	Beihilfekasse der RVK
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DS-GVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz (Arbeitsgemeinschaft der Datenschutz-Aufsichtsbehörden des Bundes und der Länder)
Düsseldorfer Kreis	Arbeitsgemeinschaft der Datenschutz-Aufsichtsbehörden des Bundes und der Länder, auch Datenschutzkonferenz (DSK)
IDM	Identity-Management/Identitätsmanagement
IFG	Informationsfreiheitsgesetz des Bundes
IFG NRW	Informationsfreiheitsgesetz NRW
LFK	Landesfamilienkasse der RVK
LVR	Landschaftsverband Rheinland Köln (www.lvr.de)
LVerbO	Landschaftsverbandsordnung für das Land Nordrhein-Westfalen
KVBbg	Kommunaler Versorgungsverband Brandenburg (www.kvbbg.de)
LDI NRW	Landesbeauftragte/r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf
MDM	Mobile Device-Management/Mobilgeräte-Management
MHKBG	Ministerium für Heimat, Kommunales, Bau und Gleichstellung NRW, Düsseldorf
MI NRW	Ministerium für Inneres NRW, Düsseldorf
RVK	Rheinische Versorgungskassen Köln (www.versorgungskassen.de)
UIG NRW	Umweltinforationsgesetz Nordrhein-Westfalen
UKlaG	Unterlassungsklagengesetz
VIG	Verbraucherinformationsgesetz
VK	Versorgungskasse der RVK
VKZVKG	Gesetz über die kommunalen Versorgungs- und Zusatzversorgungskassen im Lande Nordrhein-Westfalen vom 06.11.1984
ZVK	Zusatzversorgungskasse der RVK