Studientext Nr. 31
Stand 2026

Datenverarbeitung in der Rentenversicherung

Natalia Ruder, Michael Joachim Seeg

Deutsche Rentenversicherung
Bund

Einleitung

Allen Auszubildenden und Mitarbeiterinnen und Mitarbeitern der Aus- und Fortbildung der Rentenversicherungsträger stehen begleitend zum theoretischen Unterricht sowie zur Vertiefung und Vorbereitung auf Prüfungen zurzeit insgesamt 39 Studientexte zur Verfügung, die das prüfungsrelevante Recht der gesetzlichen Rentenversicherung abdecken und von Fachkräften der gesetzlichen Rentenversicherung erstellt wurden.

Die Studientexte eignen sich nicht nur zum Nachlesen oder zur Nacharbeit, sondern auch zum Einsatz während des Unterrichts, auch als Grundlage für Arbeitsblätter.

Selbstverständlich können auch andere Adressatenkreise (wie zum Beispiel Studierende des Studienganges Sozialversicherung (LL.B.), Inspektorenanwärter*innen, Fortzubildende sowie Sachbearbeiter*innen oder auch Rentenberater*innen) die Studientexte nutzen.

Durch ihren logischen Aufbau sowie den Einsatz vieler Beispiele und Übungen sind die Studientexte ein wertvolles Informations- und Nachschlagewerk.

Aus Gründen der besseren Lesbarkeit wird im folgenden Text weitestgehend auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter, soweit es für die Aussage erforderlich ist.

Sollten Sie aus den Studientexten zitieren, bitten wir um folgende Quellenangabe:

Studientext der Deutschen Rentenversicherung Nummer x, Titel, Autor, Ausgabe 20xx, Seite x

Eine Übersicht der verfügbaren Studientexte finden Sie am Ende dieses Studientextes.

Inhaltsverzeichnis

1. Entwicklung der Datenverarbeitung 5
   - 1.1 Historie 5
   - 1.2 Großrechner (Host) 6
   - 1.3 Personal-Computer 7
   - 1.4 Internet 8

2. Anwendungsgebiete der Datenverarbeitung in der Rentenversicherung 10
   - 2.1 Rentenversicherungssystem (rvSystem) 10
   - 2.2 Betriebswirtschaftliche Anwendungen (Systeme zur inneren Verwaltung) 11
   - 2.3 Büro- und Kommunikationssysteme 13
   - 2.4 Individualsoftware 14

3. DRV-IT 16
   - 3.1 rvDialog 16
   - 3.2 Die Gremienstruktur der DRV-IT 17
   - 3.3 Rechenzentren 23

4. Datenstelle der Rentenversicherung (DSRV) 27
   - 4.1 Rechtliche Stellung der DSRV 27
   - 4.2 Aufgaben der Datenstelle 28
     - 4.2.1 Aufgaben der DSRV als dateiführende Stelle 28
     - 4.2.2 Aufgaben der DSRV im Rahmen gesetzlichen Vorgaben 28
     - 4.2.3 Aufgaben der DSRV aufgrund Einschaltung als Vermittlungsstelle durch die Rentenversicherungsträger 29
     - 4.2.4 Aufgaben der DSRV aufgrund vertraglicher Regelungen (zum Beispiel: § 80 SGB X / § 11 BDSG) mit Rentenversicherungsträgern 29
     - 4.2.5 Aufgaben der DSRV aufgrund vertraglicher Regelungen mit Sozialversicherungsträgern 30
   - 4.3 Der Stammsatzbestand 31
   - 4.4 EU-weite Kommunikation der Sozialversicherung im Rahmen des Verfahrens EESSI 32
   - 4.5 Kommunikationspartner zu verschiedenen Stellen innerhalb und außerhalb der Sozialversicherung 34

5. Versicherungsnummer als Ordnungsbegriff 36
   - 5.1 Rechtliche Grundlagen, Sinn und Aufbau der Versicherungsnummer 36
   - 5.2 Vergabe der Versicherungsnummer 37
   - 5.3 Vergabeverfahren 38
   - 5.4 Versicherungsnummer als Basis der Krankenversichertennummer 40

6. Versicherungskonto 43
   - 6.1 Zweck des Versicherungskontos 43
   - 6.2 Rechtliche Grundlagen 43
   - 6.3 Inhalt des Versicherungskontos 44

7. Führung der Versicherungskonten, Kontoführungswechsel 46
   - 7.1 Grundsätzliches 46
   - 7.2 Zuständigkeit für die Führung von Versicherungskonten 46
   - 7.3 Kontoführungswechsel 47

8. Aktualisierung der Versicherungskonten, Meldeverfahren 51
   - 8.1 Zweck des Versicherungskontos und gesetzliche Grundlagen 51
   - 8.2 Anlässe für die Kontoaktualisierung 52
   - 8.3 Manuelle Pflege 53
   - 8.4 Elektronische Kommunikation mit anderen Stellen 53
     - 8.4.1 Meldeverfahren nach der DEÜV 54

8.4.2 Sofortmeldungen 54
8.4.3 Meldeverfahren nach BMeldDÜV 55
8.4.4 Maschinelles Meldeverfahren zur Krankenversicherung der Rentner (KVdR) und zur Pflegeversicherung 58
8.4.5 Maschinelles Erstattungsverfahren (EA – Verfahren) 58
8.4.6 Rentenzahlungen durch den Renten Service der Deutschen Post AG 59
8.4.7 Datenaustausch mit den Kliniken 60
8.4.8 Rentenbezugsmitteilungsverfahren und Maschinelles Anfrage Verfahren zur Übermittlung der steuerlichen Identifikationsnummer 60
8.4.9 Zulageverfahren Pflegeversicherung 60
8.4.10 Digitale Verfahren zur Beitragssatzdifferenzierung in der sozialen Pflegeversicherung (DaBPV) 61
8.5 Fehlerprüfung und Freigabeverfahren 62
8.6 Datenschutz 63
8.7 Datenaustausch innerhalb der Deutschen Rentenversicherung 64

9. Geschäftsprozesse und Verarbeitung der Versicherungskonten 68
9.1 Grundstruktur der Verarbeitung des Versicherungskontos 68
9.2 Geschäftsprozesse 71
9.3 Der elektronische Workflow 75
9.4 Digitales Akten-Management als Voraussetzung für Workflows 79

10. Online-Services 83
10.1 rveServices der Deutschen Rentenversicherung 83
10.2 Informationsdienste, Broschüren 84
10.3 Das Kundenportal der Deutschen Rentenversicherung 85
10.3.1 Die Online-Services ohne Identifikation 89
10.3.2 Online-Service: Antrag stellen 89
10.3.3 Online-Service: Versicherungsunterlagen anfordern 90
10.3.4 Online-Service: Persönliche Daten ändern 91
10.3.5 Online-Service: Termine vereinbaren 91
10.4 Verfahren "eSolution" der Deutschen Rentenversicherung 92
10.5 Stammsatz-Auskunft-Online 93
10.6 Elektronischer Rechtsverkehr 94
10.7 Datenaustausch im elektronischen Rechtsverkehr 95
10.7.1 eGericht 95
10.8 Zollauskunft (Beschäftigungszeiten/ A1 / Sofortmeldungen) 98
10.9 Europäisches Online Auskunftsverfahren (EOA) 99
10.10 eBanking 100
10.11 Digitale Rentenübersicht 100
10.11 Sicherheit bei Online-Services 102
10.11.1 Schutzziele und Risiko 102
10.11.2 Maßnahmen 102

11. Authentifizierung und Signatur, Datenverschlüsselung 104
11.1 Authentifizierungsverfahren 104
11.2 Elektronische Signatur 107
11.3 Datenverschlüsselung und –signierung 109
Lösungen der Aufgaben zur Selbstüberprüfung 114
Verzeichnis der Abbildungen und Tabellen 117
Verfügbare Titel der Studientext-Reihe 118
Impressum 120

1. Entwicklung der Datenverarbeitung

LERNZIELE

- Sie können die wichtigsten Entwicklungen zur Datenverarbeitung nennen und können die Einsatzbereiche der Datenverarbeitung in der Rentenversicherung erläutern.
- Sie kennen den Unterschied zwischen Batch- und Dialogverarbeitung.
- Sie können die Vorteile einer grafischen Benutzeroberfläche beschreiben.
- Sie können die Bedeutung des Internets einordnen und kennen die wichtigsten Software-Komplexe.

Die automatisierte Verarbeitung von Daten und die Unterstützung der Sachbearbeiter und Kunden durch den Computer sind heute unabdingbare Bestandteile einer modernen Verwaltung. Sie tragen zur schnellen Aufgabenerledigung bei und ermöglichen eine effiziente und effektive Bearbeitung auch in der gesetzlichen Rentenversicherung. Dabei ist uns der Umgang mit der elektronischen Datenverarbeitung schnell selbstverständlich geworden. Die Anfänge der „elektronischen Rechenmaschinen“ liegen dabei gar nicht so weit zurück. Auch die Rentenversicherung hat schnell die Vorteile dieser Technik erkannt und für sich eingesetzt.

1.1 Historie

Die heute in allen Bereichen und für die vielfältigsten Ziele eingesetzten Datenverarbeitungssysteme unterschiedlichster Leistungsstufen - vom Taschenrechner oder Spielcomputer bis hin zu den Großrechenanlagen - sind nicht das Produkt einer einmaligen Erfindung, sondern Ergebnisse einer sehr langen Entwicklung.

Riesige Rechenanlagen, die sehr störanfällig waren, stehen am Anfang der Entwicklung zu den heutigen Computern. Diese Anlagen werden heute als Computer der ersten Generation bezeichnet, weil erstmals Röhren als Schaltelemente eingesetzt wurden. Die Transistoren wurden 1947 in den Bell Laboratories der Firma AT&T erfunden. Ihr Einsatz prägt die zweite Computergeneration am Ende der 1950er Jahre. So baute IBM 1960 den 1401-Großrechner mit dieser Technik.

Miniaturisierung und Integration von Bauteilen in Modulen sind die Merkmale der dritten Computergeneration. Die Informationsmengen wurden immer größer, die elektronischen Bauteile (integrierte Schaltkreise oder englisch: *Integrated Circuit,* kurz: *IC*) immer kleiner. Und es geht noch kleiner: Hochintegrierte Schaltkreise zum Bau von Mikroprozessoren sind die Merkmale der vierten Computergeneration. Während damit einerseits Personal Computer für den heimischen Schreibtisch und den Einsatz in kleineren Betrieben konstruiert werden, brauchen Großunternehmen oder die wissenschaftlichen und militärischen Bereiche Großrechenanlagen (englisch: *Mainframes*) und Supercomputer mit enormen Rechenleistungen. In Supercomputern arbeiten mehrere Prozessoren parallel, um die gestellten Aufgaben möglichst schnell zu lösen.

1.2 Großrechner (Host)

Bereits früh bemühte sich die Verwaltung um eine Automatisierung. Nach den ersten Zählmaschinen, die 1890 bei der amerikanischen Volkszählung zum Einsatz gelangten, wurden auch die ersten Computer bald für Verwaltungstätigkeiten eingesetzt. Diese Rechnergeneration war im wahren Sinne groß, sperrig und teuer.

Unter einem Großrechner (englisch: *Mainframe*) versteht man heutzutage ein sehr komplexes und umfangreiches Computersystem. Häufig wird für Großrechner auch das Wort „Host“ (deutsch: *Wirt*, *Gastgeber*) als Synonym verwendet. Ein Großrechner zeichnet sich vor allem durch seine Zuverlässigkeit und eine hohe Ein-Ausgabe-Leistung aus. Er kann im Online-Betrieb eine große Anzahl von Benutzern bedienen, im Batch-Betrieb (siehe unten) aber auch komplizierte und aufwändige Aufgaben durchführen.

Die typischen Anwendungen eines Großrechners sind in Banken, Versicherungen, großen Unternehmen und in der öffentlichen Verwaltung gegeben. In einem Großrechner sind sorgfältig aufeinander abgestimmte, robuste und hochgradig redundante Komponenten verbaut. Üblicherweise wird die Wartung dieser Rechner im laufenden Betrieb durchgeführt. Auch Hardwareaustausch und Aufrüstungen führen zu keiner Beeinträchtigung oder gar Unterbrechung des Betriebs.

Batch- und Dialogbetrieb

Bedingt durch die sehr begrenzten Kapazitäten, die Größe der Maschinen und nicht zuletzt auch die sehr hohen Kosten waren die Datenverarbeitungsanlagen bis zu Beginn der Achtzigerjahre ausschließlich in Rechenzentren und abgeschlossenen Maschinensälen untergebracht. Dies bedeutete, dass die sachbearbeitenden Stellen nur über Datenerfassungsbelege mit den Systemen in Verbindung treten konnten. Aus dieser Zeit stammt der Begriff „Stapelverarbeitung“ (**Batch-Verarbeitung**). Programme und Datensätze wurden damals auf Lochkarten gestanzt, die Lochkarten wurden auf einen Kartenstapel (englisch: *batch*) gelegt und nacheinander abgearbeitet. Auch wenn die technischen Möglichkeiten der Stapelverarbeitung durch zusätzliche Steuerinformationen und Parameter mit der Zeit immer weiter ausgereizt wurden, bleibt eine Reihe von Nachteilen dieser Verarbeitungsart bestehen.

Die Arbeitsschritte der Stapelverarbeitung, die unvermeidlichen Wartezeiten der Bearbeiter, die Medienbrüche und die daraus resultierenden Nachteile entfallen, wenn der Bearbeiter direkt mit der Maschine und den Systemen auf Grund der gespeicherten Daten kommunizieren kann. Er kann in diesem Fall die Daten am Arbeitsplatz direkt den Verarbeitungssystemen zur Verfügung stellen, prüfen und verarbeiten lassen und auch die Ergebnisse abrufen. In gewissem Sinne tritt er damit in einen Dialog mit der Maschine ein (**Dialogverarbeitung**). Der Sachbearbeiter kann damit in einem Arbeitsschritt einen Vorgang abschließend bearbeiten, ohne die Akten mehrfach in die Hand nehmen zu müssen. Daher hat sich diese Verarbeitungsart als „Sachbearbeiterdialog“ durchgesetzt.

Aber auch noch heute hat die Batch-Verarbeitung ihren Sinn dort, wo Massendaten ohne manuellen Eingriff der Sachbearbeitung verarbeitet werden. Dies ist zum Beispiel dann der Fall, wenn viele nicht zeitkritische Informationen mit anderen Stellen ausgetauscht werden (zum Beispiel im Rahmen der DEÜV) oder eine automatische Datenspeicherung im Versicherungskonto (siehe Kapitel 6) erfolgt.

1.3 Personal-Computer

Waren zunächst am Arbeitsplatz der Sachbearbeitung fast ausschließlich „dumme“ Datensichtgeräte im Einsatz, so sind heute fast durchgängig intelligente Personal Computer zu finden, die durch zusätzliche Anwendungen und Standardprogramme (zum Beispiel Office-Pakete) einen Zusatznutzen auf den Schreibtisch bringen. Ein **Personal Computer** (deutsch: *persönlicher Computer*; kurz PC), ist ein Einzelplatzrechner, der im Gegensatz zu einem Großrechner von einer einzelnen Person (daher persönlich) bedient, genutzt und gesteuert werden kann. Den Personal Computer in heutiger Form gibt es seit den frühen 1980er Jahren. Er hat sich mit seinen Bedienelementen, wie Tastatur und Maus sowie farbigem Bildschirm mit einer GUI (englisch: *Graphical User Interface; deutsch: grafische Benutzeroberfläche*), an unseren Büroarbeitsplätzen durchgesetzt.

Eine **grafische Benutzeroberfläche** ist eine Softwarekomponente, die einem Computerbenutzer die Interaktion mit der Maschine über grafische, metapherhafte Elemente (Symbole, Papierkorb, Menü) unter Verwendung eines Zeigegerätes, wie einer Maus, erlaubt. Die Bewegung der (Computer-) Maus auf der Unterlage wird über einen Sensor in der Mausaufgenommen und an den angeschlossenen Computer übertragen. Über Funktionen des Betriebssystems wird diese zweidimensionale Bewegungsinformation in eine gleichartige Bewegung des Mauszeigers (umgangssprachlich „*Cursor*“) auf dem Bildschirm umgesetzt. Durch Betätigung der Tasten (Klick, Doppelklick) oder zusätzlicher Elemente der Maus kann der Nutzer verschiedene Aktionen in dem Betriebssystem oder dem Anwendungsprogramm ausführen.

Die Einführung der Computermaus kann als ein entscheidender Durchbruch in der Verbesserung der Benutzerfreundlichkeit von Computern angesehen werden. Seit Mitte der 1980 bildet die Maus somit für fast alle Computertätigkeiten zusammen mit dem Monitor und der Tastatur die Mensch-Maschine-Schnittstelle. Für diese neuen grafischen Oberflächen wurden dann diverse Regeln geschaffen und verschiedene Zielvorstellungen — beispielsweise intuitive Bedienbarkeit — definiert. Durch Firmen wie Apple oder Microsoft haben sich grafische Benutzeroberflächen schnell verbreitet und sind heute Standard.

Grafische Benutzeroberflächen haben auch in die zentral zur Verfügung gestellten Großrechneranwendungen Eingang gefunden, mit denen heute über den PC und sogenannten Host-Emulationen gearbeitet wird. Die Vorteile dieser neuen Darstellung liegen insbesondere im Bedienungs-Komfort für den Endbenutzer. Durch die Einbeziehung diverser Hilfefunktionen und Menü-Techniken wird die Einarbeitungszeit der Sachbearbeitung auch bei neuen Funktionen verkürzt. Gleichzeitig ermöglicht diese Systemunterstützung weitgehend den Verzicht auf manuelle Schlüsselverzeichnisse, Benutzerhandbücher und dergleichen. Somit muss heute niemand mehr EDV-Spezialist sein, um eine Anwendung nutzen zu können.

Die ersten **individuellen Datenverarbeitungsprogramme** auf dem PC fasst man heute unter dem Begriff „Büroanwendung“ zusammen. Schreib- oder Textverarbeitungsprogramme brachten die Personal Computer nicht nur ins Büro, sondern auch zu vielen Privatanwendern.
Elektronische Tabellen, Datenbanken und Grafikprogramme runden den Einsatz als Office-Anwendung ab. Daneben gibt es heute keinen Anwendungsbereich, der nicht durch entsprechende PCs und PC-Software unterstützt würde. Die Palette reicht von der Finanzbuchhaltung bis zum Architekturprogramm. Wer kann, kann seine Programme in zahlreichen Programmiersprachen und mit grafischen Tools selbst erstellen und anpassen.

Bedeutung hat der Personal Computer in der öffentlichen Verwaltung auch, weil er über Browser den Zugriff auf das Internet ermöglicht.

1.4 Internet

Der rasende Fortschritt in den letzten Jahren im Bereich der Telekommunikation und Informationstechnologie hat nicht nur die kühnsten Erwartungen übertroffen, sondern eröffnet auch ein breites Feld an neuen Möglichkeiten. Von allgemeinen Informationsangeboten über zielgruppenorientierte Hinweise (zum Beispiel für Versicherte, Rentner oder Selbstständige) bis zu interaktiven Serviceleistungen ist heute alles über das Internet verfügbar.

Das Internet, wie wir es heute kennen, hat seine Ursprünge im Jahr 1969 und entwickelte sich rasch von einem Laborexperiment zu einem funktionsfähigen System, in dem verschiedenartige Computersysteme miteinander verbunden waren und der Austausch von Daten auf einfache Art und Weise möglich wurde. In den nächsten Jahren mussten die Kommunikationsprotokolle und Datenverbindungen mit den unterschiedlichen Hardwarearchitekturen der Hersteller in Einklang gebracht werden. Der wichtigste Schritt in diese Richtung war die Implementierung von Transmission Control Protocol beziehungsweise Internet Protocol (TCP/IP), mit dem es möglich wurde, eigenständige Netzwerke miteinander zu verbinden.

Ende der 1980er Jahre entstand auch das **World Wide Web** (WWW) als der heute populärste Teil des Internets. Die Popularität des WWW stieg vor allem durch die Einführung des WWW-Browsers „Mosaic“ im Jahr 1993. Dieser und andere einfach zu bedienende Darstellungsprogramme machten das Internet für die breite Masse zugänglich. Neben den sinkenden Telekommunikationskosten, der breiten Verfügbarkeit von Internetanschlüssen und dem einfachen Zugang über Browser hat insbesondere das immer noch stetig steigende Informationsangebot das Internet so populär gemacht. Dabei ergibt sich die Beliebtheit des Internets im Wesentlichen aus der Nutzung einiger, weniger Dienste. So haben die Dienste „E-Mail" und „World Wide Web“ (WWW) aktuell die größte Bedeutung.

Zum Informationsaustausch zwischen Personen wurden recht früh Anwendungen und die erforderlichen Kommunikationsprotokolle für den Austausch von elektronischer Post (**E-Mail**) entwickelt. Die Anwendungen bestehen aus zwei Teilen: Mailservern und Mailclients. Mail-clients werden vom Benutzer zum Erstellen, Versenden und Lesen von E-Mails verwendet. Die Mailserver übernehmen die Verteilung der E-Mails durch das Internet, nehmen E-Mails eines Benutzers entgegen und bewahren diese auf, auch wenn der Benutzer selbst gerade nicht anwesend ist.

Von WWW-Servern können die verschiedensten Daten aus der ganzen Welt abgerufen, verwaltet oder verändert werden. Komplexe Anwendungen, wie zum Beispiel im E-Government oder beim Online-Banking, können WWW-basiert bereitgestellt werden. Service-Leistungen von Behörden sind heute vielerorts bereits online verfügbar — auch die Deutsche Rentenversicherung ist mit zahlreichen Dienstleistungen im Web vertreten.

Viele Firmen haben die Internet-Technologie für sich entdeckt, um die interne Kommunikation und Information zu verbessern. Sie nutzen dabei für ihr internes Informations- und Kommunikationsnetz (**Intranet**) das gleiche Prinzip und die gleiche Technik wie für das öffentliche Internet. Ein Intranet ist aber vom Internet abgekoppelt und nur einer begrenzten Benutzergruppe zugänglich.

ZUSAMMENFASSUNG

- In Kapitel 1 haben wir gesehen, wie die Informations- und Kommunikationstechnik weite Teile unseres Lebens bestimmt. Während in den öffentlichen Verwaltungen Großrechnersysteme die Arbeiten im Hintergrund unterstützen, hat sich der Personal Computer durch seine leichte Bedienbarkeit an den Arbeitsplätzen durchgesetzt. Internet und Intranet gehören heute selbstverständlich sowohl zum privaten wie zum beruflichen Umfeld.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

1. Durch welches Merkmal werden die Computer-Generationen bestimmt?

2. Welche Art der Verarbeitung wird heute für die Sachbearbeitung überwiegend eingesetzt?

3. Nennen Sie die Hauptvorteile, die die Dialogverarbeitung gegenüber der Stapelverarbeitung hat.

4. Worin unterscheiden sich Internet und Intranet und was haben sie gemeinsam?

2. Anwendungsgebiete der Datenverarbeitung in der Rentenversicherung

LERNZIELE

- Sie kennen die wesentlichen Funktionen eines Rentenversicherungssystems.
- Sie können andere wesentliche Anwendungsgebiete der Datenverarbeitung in der Rentenversicherung nennen.
- Sie kennen die Haupteinsatzgebiete von HCL Notes in der Rentenversicherung.
- Sie kennen den Unterschied zwischen Standard- und Individualsoftware und können die Vor- und Nachteile der jeweiligen Lösung beschreiben.

In Kapitel eins wurde bereits ausgeführt, wie die elektronische Datenverarbeitung fast jeden Bereich unseres Umfeldes erreicht hat. Dies trifft auch auf die maschinelle Unterstützung aller Arbeiten in der gesetzlichen Rentenversicherung zu. Auf Grund der weitreichenden und komplexen Funktionalität jedes einzelnen Systems würde eine vollständige, detaillierte Betrachtung den Rahmen dieses Studientextes überschreiten. In diesem Kapitel erhalten Sie daher nur einen Überblick über die Anwendungsbereiche der Datenverarbeitung in der Rentenversicherung.

Die wichtigste Anwendung in der deutschen Rentenversicherung ist das Rentenversicherungssystem, mit dem die anfallenden Rentenfachverfahren bedient werden. Daneben wird Datenverarbeitung in vielen betriebswirtschaftlichen Bereichen, von der Personalwirtschaft bis zur Lagerverwaltung genutzt. E-Mail- und Büroanwendungen sowie sonstige Standardsoftware bilden einen weiteren Anwendungsbereich. Nicht zuletzt sind zahlreiche individuell entwickelte Programme im Einsatz.

2.1 Rentenversicherungssystem (rvSystem)

Das derzeitige Arbeitsprogramm in der Sachbearbeitung „rvDialog“ als Teil des rvSystems ist die Hauptanwendung in der Rentenversicherung. Hiermit werden alle direkt oder indirekt aus dem Beitrags-, Rehabilitations- und Rentenrecht sowie den tangierenden Vorschriften resultierenden Aufgaben und Arbeiten abgedeckt. Die Masse der Mitarbeitenden bei den Rentenversicherungsträgern arbeitet daher mit diesem System. Der Begriff „**rvDialog“** soll den Austausch von Daten und Informationen in einem einheitlichen Programmsystem symbolisieren. Er steht auch für die Kommunikation zwischen den Rentenversicherungsträgern.

Aus der Vielfalt aller integrierten Funktionen, die in den Kapiteln fünf ff. näher erläutert werden, sollen nachfolgend stichwortartig nur die wichtigsten genannt werden:

- Eröffnen von Versicherungskonten nach Vergabe der Versicherungsnummer,
- Führung und Aktualisierung der Versicherungskonten inklusive Beitragseinzug für Selbstzahler,
- Erteilung von Auskünften aus dem Versicherungskonto,
- Ermittlung, Bewilligung und Zahlung von Leistungen,
- Zahlungsverkehr über den Postrentendienst sowie Banken,
- Erstellung statistischer Basisdaten.

Schon hier ist erkennbar, dass das **Versicherungskonto** die zentrale Datensammlung für alle Funktionen ist. Daher sind neben den persönlichen Daten auch das gesamte Versicherungsleben sowie alle Leistungsdaten hier gespeichert. Das Versicherungskonto wird im Kapitel sechs näher erläutert.

Ebenso wird klar, welchen immensen Funktionsumfang das rvSystem haben muss. Es ist aber nur für den Kreis der Rentenversicherungsträger anwendbar. Standard- oder Branchensoftware ist für diesen Anwendungsbereich nicht erhältlich. Daher werden alle erforderlichen Programme von den Trägern der Rentenversicherung selbst entwickelt und gepflegt.

2.2 Betriebswirtschaftliche Anwendungen (Systeme zur inneren Verwaltung)

Die Rentenversicherungsträger sind Selbstverwaltungskörperschaften mit eigener Personal- und Finanzhoheit. Sie müssen zur Aufrechterhaltung des Dienstbetriebes eigene Personal-, Finanz- und Materialverwaltungsabteilungen unterhalten. Zudem führen sie mit den Kliniken, Untersuchungsstellen u. ä. sogenannte Eigenbetriebe mit einem eigenen Aufgabenspektrum. Neben der Hauptanwendung, dem rvSystem, sind bei den Rentenversicherungsträgern deshalb auch Systeme zur Unterstützung der inneren Verwaltung installiert.

In der **Personalverwaltung** sind beispielsweise verschiedene Anwendungsbereiche zu unterscheiden, die teilweise aus Gründen des Datenschutzes keine datentechnischen Verbindungen untereinander haben dürfen. Im Einzelnen sind hier zu nennen:

- Lohn- und Gehaltsabrechnungssysteme (Berechnung der Löhne und Gehälter, Erstellung der Festsetzungen, Führung maschineller Lohnkonten, Jahresabrechnungen, Erstellung von Entgeltmeldungen sowie Abrechnung von Sozialbeiträgen und Lohnsteuer),
- Zeiterfassungssysteme (Gleitzeit, Urlaub, Krankheit) sowie
- Personaldatensysteme (Führung aktueller Personal- und Stellenplandaten für Personalplanung, Terminwahrnehmung, Erstellung von Telefonverzeichnissen, Unterstützung von Controllingaufgaben).

Die **Finanzverwaltungssysteme** unterstützen weitgehend den gesamten Bereich der in der Finanzverwaltung anfallenden Arbeiten, wie insbesondere:

- das tägliche Buchen und Zahlen,
- die Tages-, Monats- und Jahresabschlüsse,
- die Führung von Nebenbuchhaltungen für Wertpapiere, Darlehen, Mieten, Pachten, Debitoren, Kreditoren und so weiter,
- die Erstellung von Haushaltsplänen sowie
- die Führung einer Kostenstellenrechnung.

Die einzelnen Versicherungsträger haben einen großen Bestand an Immobilien und Inventar. Außerdem werden Büromaterialien verbraucht. Hier sind erhebliche finanzielle Mittel im Einsatz, die es erforderlich machen, das vorhandene sowie das zu beschaffende Material beziehungsweise die Anlagen nicht nur nachprüfbar, sondern auch effizient und wirtschaftlich zu beschaffen und zu verwalten. Im Rahmen der allgemeinen Verwaltung werden daher von Material- und **Anlagenwirtschaftssystemen**

- die Lagerhaltung und -überwachung,
- das Bestellwesen,
- die Abrechnung mit Lieferanten und Abnehmern,
- die Apotheken der Kliniken sowie
- die Angebotsvergleiche

maschinell unterstützt.

Die Träger der Rentenversicherung unterhalten zur Durchführung der medizinischen Rehabilitation eigene Kliniken. In diesen Häusern, die teilweise auch Krankenhauscharakter haben und mit Ambulanzen beziehungsweise Akutmedizin ausgestattet sind, stehen neben den Pflegefachbereichen auch die zugehörigen Funktionsbereiche wie Therapie, Diagnostik, Apotheke und so weiter zur Verfügung.

Ein nicht unwesentlicher Teil der Datenverarbeitungssysteme der Rentenversicherungsträger ist daher auf eine möglichst umfassende Unterstützung der Kliniken (**Kliniksoftware**) ausgerichtet.

Aus Gründen des Datenschutzes ist eine saubere Trennung zwischen Verwaltungsdaten und medizinischen Informationen auch datenverarbeitungstechnisch unverzichtbar.

2.3 Büro- und Kommunikationssysteme

Diese reinen Fachanwendungen unterstützen die Arbeit der Sachbearbeitung in den Fach- und Verwaltungsbereichen. Daneben sind jedoch bei den Rentenversicherungsträgern noch eine Vielzahl allgemeiner Büro- und Kommunikationsaufgaben abzudecken, die im Interesse einer wirtschaftlichen und rationellen Aufgabenerledigung ebenfalls einer maschinellen Unterstützung bedürfen.

Auch hier gilt natürlich, dass die eingesetzten Systeme und Geräte je nach interner Organisationsform unterschiedlich sind. So werden die nachfolgend aufgeführten Anwendungen teilweise von stationären Personal Computern (PCs), Notebooks, Bürosystemen oder auch Mehrplatzsystemen abgedeckt. Unterschiedlich sind ebenso die Hersteller, die Betriebssysteme sowie die Art und Weise der Vernetzung.

Nachfolgend werden daher lediglich zur Übersicht die hauptsächlichen Anwendungen im Büro- und Kommunikationsbereich aufgezeigt:

- Textbe- und Verarbeitungssysteme für die Schreibdienste und Sekretariate,
- Tabellenverarbeitung zur Aufbereitung von statistischen Auswertungen,
- Grafiksysteme zur Visualisierung von Statistiken und Erstellung freier grafischer Darstellungen,
- Desktoppublishing-Systeme (zum Beispiel zur Erstellung von Broschüren; ggf. direkte Weitergabe an Satzsysteme der Druckereien) zur Öffentlichkeitsarbeit und Herstellung von Formblättern,
- Datenbanksysteme zur individuellen Speicherung von Informationen, zum Beispiel Adressen für Serienbriefe,
- Kommunikationssysteme (Mailbox, Datenaustausch und so weiter) zur Hinterlegung von Nachrichten und Austausch von Informationen,
- Informationsspeicher- und Suchsysteme (Retrieval-Systeme), beispielsweise zur strukturierten Speicherung von Dienstanweisungen und Zugriff über Schlagworte.

Für die interne und externe Kommunikation über E-Mail (ein sogenannter Social-Business-Client) hat sich in der Rentenversicherung das System „**HCL Notes“** verbreitet. Damit lässt sich nicht nur der Mailverkehr abwickeln, sondern Notes integriert auch Informationsdatenbanken unterschiedlichster Art (zum Beispiel eine zentral geführte Notes-Datenbank mit allen Gremienvorlagen und -niederschriften oder Arbeitsanweisungen und Hausverfügungen). Es bietet auch Chat-Funktionen (*Instant Messaging*) zur unmittelbaren Kommunikation sowie über das Zusatzprodukt „Sametime“ Werkzeuge zur Zusammenarbeit (englisch: *Collaboration Tools*) wie gemeinsame Bearbeitung von Dokumenten bis zu Audio- und Video-Konferenzen an. Der Einsatz dieser Tools orientiert sich dabei an den Hausregelungen und dem zu erreichenden Nutzen.

2.4 Individualsoftware

Als **Standardsoftware** werden Softwaresysteme verstanden, die einen klar definierten Anwendungsbereich abdecken und als vorgefertigte Produkte erworben werden können. **Individualsoftware** hingegen zeichnet sich dadurch aus, dass sie gemäß den Anforderungen eines einzelnen Kunden maßgeschneidert erstellt wird.

Zu den wichtigsten Anwendern von Individuallösungen zählen große Behörden und vergleichbare Einrichtungen, da aufgrund der Vielfalt und Änderungshäufigkeit von gesetzlichen Vorschriften, Verantwortlichkeiten und politischen Interessen nur selten exakt passende marktgängige Softwareprodukte verfügbar sind. Dies trifft beispielsweise auch auf die Rentenversicherungssysteme zu.

Vor- und Nachteile von Standardsoftware gegenüber Individualsoftware

Grundsätzlich hängt es vom konkreten Fall ab, ob der Einsatz von Standard- oder Individualsoftware günstiger ist. Als Hauptvorteil des Einsatzes von Standardsoftware werden meist die geringeren Kosten genannt, was sich allerdings häufig aufgrund erforderlicher Anpassungen (Konfiguration) an vorhandene Systembestandteile relativiert. Die Möglichkeit des Zuschneidens auf die individuellen Gegebenheiten wird häufig als Hauptargument für den Einsatz von Individualsoftware angeführt. In vielen Fällen ist es nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, Standardsoftware einzusetzen. Insbesondere, wenn sehr spezielle Anforderungen hinsichtlich vorhandener Infrastruktur bestehen (etwa, weil viele Schnittstellen zu Fremdsystemen zu berücksichtigen sind) oder sehr spezielle und komplexe Geschäftsprozesse abgebildet werden müssen, ist die Implementierung von Individualsoftware oftmals unumgänglich. Hinzu kommt gerade in der öffentlichen Verwaltung der Wunsch, eine vollkommene Kontrolle über die künftige Entwicklung der Software und die Beherrschung des Quellcodes zu garantieren. In der Industrie soll eine Individualsoftware dem einsetzenden Unternehmen gegenüber anderen Mitbewerbern einen Wettbewerbsvorteil verschaffen.

Für den Einsatz von Standardsoftware sprechen hingegen, dass der Aufbau und die Aktualisierung von Know-how in einem speziellen Fachgebiet (zum Beispiel Finanzen) für den Hersteller einer weitverbreiteten Standardsoftware einfacher und lohnender, als für Entwickler einer Individualsoftware ist. Außerdem können neue Mitarbeitende eines Unternehmens bei einem hohen Verbreitungsgrad einer Standardsoftware (zum Beispiel einer Textverarbeitung) bereits Kenntnisse eingesetzter Standardsoftware mitbringen.

In der Deutschen Rentenversicherung wird vor allem bei betriebswirtschaftlichen Anwendungen Standardsoftware zum Beispiel von SAP oder Wilken eingesetzt. Im Bereich der Office-Produkte erfreut sich das Office-Paket der Firma Microsoft großer Verbreitung.

Das Rentenversicherungssystem selbst wird aus den oben genannten Gründen von den Rentenversicherungsträgern eigens entwickelt. Eigenentwicklungen sind beispielsweise auch für die Unterstützung der Prüfdienste auf mobilen Rechnern im Einsatz. Diese helfen den Betriebs- und Einzugsstellenprüfern vor Ort bei der Prüfung durch die Anzeige von rentenversicherungsinternen Prüfhilfelisten, bei der Nachberechnung von Beiträgen durch entsprechende Beitragsrechner sowie durch eine Textverarbeitung mit passenden Textbausteinen bei der Abfassung des Prüfberichtes. Der Vorteil dieser Individualsoftware liegt neben der Integration der Anwendungen in die Geschäftsprozesse, die in der Hauptverwaltung vorausgehen oder sich anschließen, in der Fokussierung der Software auf die Bedürfnisse der Benutzer (Textbausteine gegenüber komplexem Textsystem) sowie der höheren Flexibilität, mit der auf Wünsche der Anwender oder gesetzliche Änderungen reagiert werden kann.

ZUSAMMENFASSUNG

- In Kapitel 2 wurde die bereits Eingangs getroffene Feststellung, wonach es bei den Rentenversicherungsträgern keinen Bereich mehr gibt, der nicht von den maschinellen Systemen direkt oder indirekt beeinflusst ist, näher erläutert und bewiesen. Es ist aber auch deutlich geworden, dass die Versicherungsträger, vor allem wegen der sehr heterogenen Größen und Organisationsformen, bislang keine Einheitlichkeit bei den Systemen zur inneren Verwaltung sowie den Büro- und Kommunikationssystemen haben können.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

5. Nennen Sie die Hauptanwendung der Rentenversicherung.

6. Zählen Sie einige Systeme zur inneren Verwaltung auf.

7. Welche Systeme sind ergänzend zu den Fachsystemen vorhanden?

8. Welches sind die Hauptfunktionen von HCL Notes?

9. Beschreiben Sie Vor- und Nachteile von individuell erstellter Software.

3. DRV-IT

LERNZIELE

- Sie kennen den Zweck der Zusammenarbeit der Träger der Rentenversicherung in der DRV-IT und deren wichtigste Gremien.
- Sie können die Ziele der Neuentwicklung in rvDialog benennen.
- Sie wissen über die Bedeutung der Rechenzentren und des Datennetzes für die Aufgabenerledigung der DRV-IT Bescheid.

Wie Sie bereits wissen, sind die Träger der Rentenversicherung selbstverwaltete, eigenständige Organisationen. Dies bedeutet auch, dass die Träger Umfang und Einsatz der Datenverarbeitung jeweils selbst bestimmen können. Allerdings ist die Realisierung und Pflege eines Rentenversicherungssystems des angedeuteten Leistungsumfanges so arbeitsintensiv, dass der Datenverarbeitungs-Bereich eines einzelnen Rentenversicherungsträgers die Aufgaben allein nur schwer bewältigen könnte. Die Versicherungsträger hatten sich daher zur arbeitsteiligen Erstellung und Pflege des rvSystems in **Programmierkreise** zusammengeschlossen. So hatten sich innerhalb der Rentenversicherung bereits in den Siebzigerjahren vier Programmierkreise gebildet, die jeweils gemeinsam für mehrere Rentenversicherungsträger die Programmentwicklung durchführten.

Im Rahmen interner Organisationsreformen hatten sich bereits der ehemalige Programmierkreis „Verband Deutscher Rentenversicherungsträger“ (VDR), der Süddeutsche Programmierkreis und der Westdeutsche Programmierkreis zum „Arbeitskreis für Informationstechnologie” (**AKIT**), in dem die Regionalträger der Deutschen Rentenversicherung und die Deutsche Rentenversicherung Knappschaft-Bahn-See (DRV KBS) vertreten waren, zusammengeschlossen. Ziel dieses Programmierkreises war es, unter anderem arbeitsteilig für alle beteiligten Versicherungsträger das „gemeinsame Rentenversicherungssystem“ (GRVS) zu entwickeln und weiterzupflegen. Ab 2010 wurden sukzessive das Programmsystem rvGlobal® der Deutschen Rentenversicherung Bund und das Rentenversicherungssystem GRVS der übrigen Versicherungsträger zu einem gemeinsamen neuen Kernsystem rvDialog zusammengeführt.

3.1 rvDialog

Die Erstellung und Weiterentwicklung von rvDialog erfolgte in mehreren Abschnitten. Nach der Konzeptionsphase erfolgte in der Migrationsphase der Aufbau einer technisch ablauffähigen Programmversion, die um erforderliche Funktionen ergänzt wurde. Am Ende des Abschnitts zwei stand die produktionsreife Programmversion rvDialog 2.000. Diese wurde seit Frühjahr 2013 bei den Regionalträgern und der DRV Knappschaft-Bahn-See eingesetzt. Die DRV Bund hat im August 2013 mit der schrittweisen Migration ihrer Arbeitsplätze auf rvDialog begonnen. Ende 2017 waren alle Versicherungskonten umgestellt.

Nach der Produktivsetzung von rvDialog liegt der Schwerpunkt der Modernisierung und Weiterentwicklung des gemeinsamen Programmsystems auf den Effekten der Automatisierung und Optimierung. Insbesondere durch die Einführung / Ausweitung des elektronischen Dokumentenworkflows zur Digitalisierung der Geschäftsprozesse werden weitere Synergieeffekte erwartet.

3.2 Die Gremienstruktur der DRV-IT

Als Folge der Organisationsreform im Jahr 2005 haben sich alle Träger zur Verstärkung der Zusammenarbeit auf dem Gebiet der Informationstechnologie zur „DRV-IT“ zusammengeschlossen. Die Grundlagen der Zusammenarbeit sind in der „Vereinbarung über die Zusammenarbeit der Rentenversicherungsträger im Bereich der Informations- und Kommunikationstechnik“ (Vereinbarung IuK) geregelt.
Die DRV-IT fühlt sich dabei folgenden Zielen der Deutschen Rentenversicherung im Bereich der Informations- und Kommunikationstechnik verpflichtet:

- **Kundenorientierung**
  Die Bedarfe der externen Kund*innen sowie der sie betreuenden Rentenversicherungsträger sind der Maßstab für die Erbringung der IT-Services. Umfasst werden davon auch diejenigen Bedarfe dritter Stellen, die an der Leistungserbringung gegenüber den/der externen Kund*innen der Deutschen Rentenversicherung mitwirken und aus diesem Grund ebenfalls Anforderungen an den Service der Deutschen Rentenversicherung stellen. Die angebotenen Services unterstützen die Geschäftsprozesse in der Deutschen Rentenversicherung.

- **Qualität**
  Die angebotenen Services sind von hoher Qualität

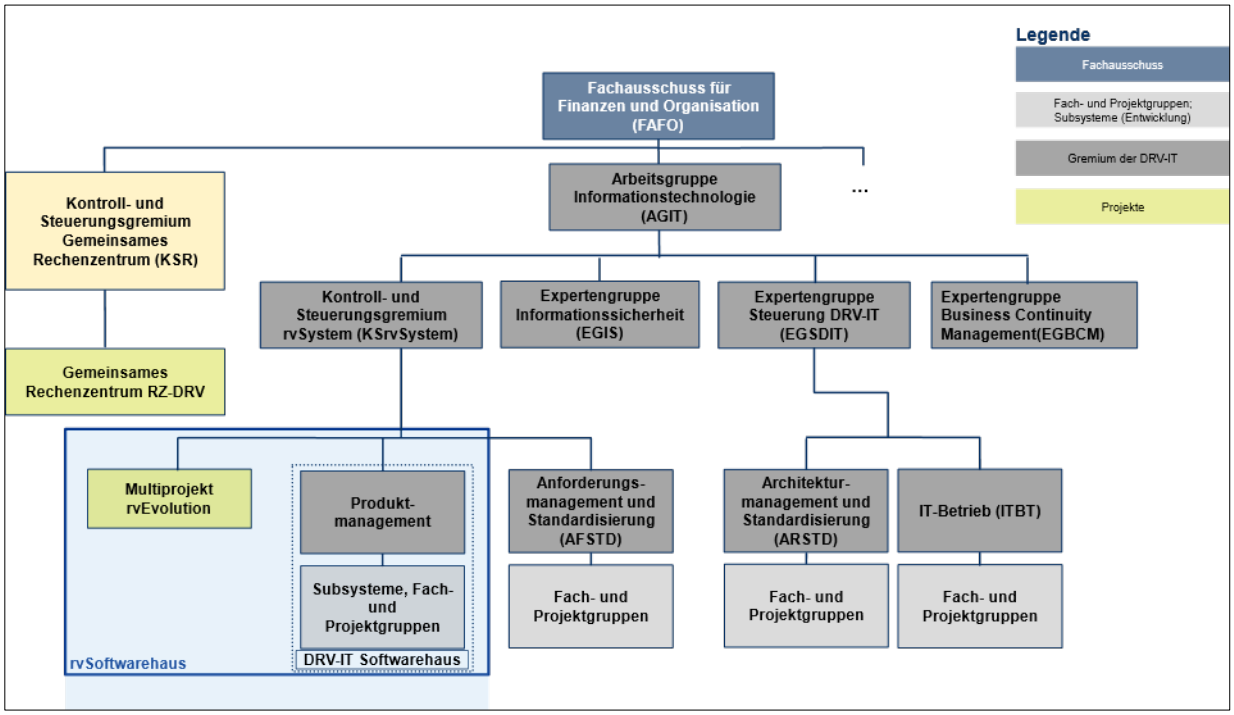
- **Wirtschaftlichkeit**
  Die angebotenen Services werden in einem angemessenen Kosten- / Nutzenverhältnis erbracht.

- **Mitarbeiter*innen**
  Die Mitarbeiter*innen in der DRV-IT der Deutschen Rentenversicherung sind gut ausgebildet und werden zielgerichtet fortgebildet.

Das gemeinsame Ziel der DRV-IT ist es, den Trägern der Deutschen Rentenversicherung eine wirtschaftliche IT von hoher Qualität anzubieten, welche die Ressourcen der gesamten DRV optimal nutzt.

Gremien
Zur Abstimmung und Entscheidung aller in der DRV-IT zu behandelnden Themen wurde eine Gremienstruktur aufgebaut. Diese stellt sich seit 2025 wie nachfolgend dar; die Gremien sind trägerübergreifend besetzt.

Abbildung 1: Gremienstruktur der DRV-IT



Fachausschuss für Finanzen und Organisation (FAFO):
Oberstes Entscheidungsgremium für die DRV-IT ist der FAFO als „Vollversammlung“ aller Träger, vertreten durch die jeweiligen Geschäftsführenden. Fachausschüsse haben die Aufgabe, in Sach- und Rechtsfragen eine gemeinsame Willensbildung und eine einheitliche Verfahrensweise bei den Rentenversicherungsträgern sicherzustellen und den Bundesvorstand durch Stellungnahmen zu beraten. Sie haben außerdem die Aufgabe, verbindliche Entscheidungen zu Grundsatz- und Querschnittsaufgaben und Entscheidungen in gemeinsamen Angelegenheiten der Träger der Rentenversicherung vorzubereiten und ist zuständig für Fragen mit strategischer und sonstiger erheblicher Bedeutung. Weiter hat der zuständige Fachausschuss die Aufgabe, die operative Kontrolle und Steuerung des Gemeinsamen Rechenzentrums nach § 51 Absatz 2 Ziffer 17 der Satzung der Deutschen Rentenversicherung Bund sicher zu stellen. Zur Erfüllung dieser Aufgabe setzte der zuständige FAFO ein **Kontroll- und Steuerungsgremium für das Gemeinsame Rechenzentrum (KSR)** ein.

Der FAFO ist kein Gremium der DRV-IT. Als übergeordnetes Gremium der Arbeitsgruppe Informationstechnologie entscheidet der FAFO jedoch in Bezug auf die Aufgaben der DRV-IT, insbesondere über:
1. die Fortschreibung einschließlich der Konkretisierung der Vereinbarung IuK;
2. die Übertragung von Aufgaben;
3. die Delegation von Entscheidungsbefugnissen an die Arbeitsgruppe Informationstechnologie;
4. die Wahl des/der Vorsitzenden der Arbeitsgruppe Informationstechnologie;
5. Kosten und Vorschüsse.

Arbeitsgruppe Informationstechnologie (AGIT):
Die AGIT wurde durch den FAFO eingesetzt, um u.a. folgende Aufgaben wahrzunehmen:

- Vorbereiten von grundlegenden strategischen Entscheidungen sowie Investitionsentscheidungen zur DRV-IT durch den FAFO im Bereich der Informations- und Kommunikationstechnologie;
- Treffen von Festlegungen zur Umsetzung der grundlegenden IT-Strategie durch (trägerübergreifende) Beschaffung, Eigenentwicklung und Betrieb der IT einschließlich der Priorisierung;
- Genehmigen von IT-Rahmenkonzepten und deren Finanzplanung;

- Steuern der Umsetzung von Konzepten zur technischen Optimierung und Automatisierung von Geschäftsprozessen;
- Festlegen von IT-bezogenen Qualitäts- und Sicherheitsstandards;
- Steuern der Umsetzung der Informationssicherheits-Policy;
- Entscheiden über die Entwicklung und Beschaffung von Software ab den relevanten Schwellenwerten gemäß den Regelungen der DRV-IT;
- Treffen von strategischen Entscheidungen zum Modernisieren, Weiterentwickeln und Standardisieren von Hard- und Software;
- Steuern der Errichtung und des Betriebs des Gemeinsamen Rechenzentrums der DRV, soweit nicht grundlegende strategische Festlegungen (zum Beispiel Ausgestaltung des Partizipationsmodells, Festlegung des Personalkonzeptes, Haushaltsaufstellung) betroffen sind;
- Ausgestalten, Ausführen und Nachhalten von Beschlüssen der Selbstverwaltungsgremien, des Erweiterten Direktoriums und der Fachausschüsse;
- Beraten von Stellungnahmen (soweit der Aufgabenbereich der Besonderen Arbeitsgruppe tangiert ist) zu Prüfungen und Anfragen der Rechtsaufsicht, des Bundesrechnungshofes sowie weiterer Prüf- und Kontrolleinrichtungen, die mehrere Rentenversicherungsträger betreffen, und Erarbeiten von Vorschlägen über Konsequenzen aus diesen Prüfungen / Anfragen.

Damit verantwortet die AGIT mit insgesamt acht Geschäftsführern (zwei Geschäftsführer der DRV Bund, fünf Geschäftsführer von den Regionalträgern und ein Geschäftsführer der DRV KBS) die Strategie der DRV-IT.

Die von der AGIT eingesetzten Gremien (Expertengruppe „Informationssicherheit“ (EGIS), Expertengruppe „Business Continuity Management“ (EGBCM), Expertengruppe „Steuerung DRV-IT“ (EGSDIT) und das Kontroll- und Steuerungsgremium rvSystem (KS rvSystem) stellen den Praxisbezug her und liefern Argumente für oder gegen Entscheidungen der AGIT.
Das gemeinsame Ziel der Gremienarbeit besteht darin, die DRV IT weiterzuentwickeln und gut für die Zukunft aufzustellen. Neben der IT-Sicherheit und dem Business Continuity Management geht es vor allem um Entwicklungen im trägerübergreifenden Softwaresystems rvSystem.

Expertengruppe Business Continuity Management (EGBCM)
Die EGBCM, bestehen aus den Notfallbeauftragten der DRV, hat unter anderem folgende Aufgaben:

- Übergeordnete Koordination des Business Continuity Managements
- Notfallabsicherung von rvSystem beziehungsweise des Leistungssystems
- Festlegung eines gemeinsamen Tools für das Business Continuity Management
- Gemeinsame koordinierte Planung eines übergreifenden Notfallmanagements zur Sicherstellung der KRITIS-Anforderungen für den RZ-Ausfall (insbesondere RZ-RV).

„**Expertengruppe Informationssicherheit“ (EGIS)**
Die Expertengruppe Informationssicherheit (EGIS), besetzt mit den IT-Sicherheitsbeauftragten der DRV, ist zuständig für folgende Aufgaben:

- Weiterentwicklung, Aktualisierung und Pflege der Informationssicherheits-Policy der DRV (ISP) gegebenenfalls in Abstimmung mit der Arbeitsgruppe Geheimnis- und Datenschutz (AGGDS), soweit datenschutzrechtliche Aspekte betroffen sind;
- Erstellen von Richtlinien (ISP Ebene 3) und trägerübergreifenden Konzepten (ISP Ebene 4) zur IT-Sicherheit, diese werden zur Entscheidung und weiteren Veranlassung der AGIT vorgelegt;
- Begleiten der Umsetzung von Konzepten zur IT-Sicherheit von DRV-weiten Projekten;
- Beraten und abschließende Entscheidung von Vorgaben für IT-Sicherheitskonzepte;

- Beraten und abschließende Entscheidung von Vorgaben für das zentrale ISM-Tool der DRV;
- Ausgestalten, Ausführen und Nachhalten von Beschlüssen der EGIS in den jeweiligen Regionen;
- Planen von Maßnahmen zur Erfüllung der BSI-Kritisverordnung und zur Erfüllung des branchenspezifischen Sicherheitsstandards B3S;
- Unterstützen des/der IT-Sicherheitsbeauftragten der DRV bei Stellungnahmen und der Begleitung von DRV-IT weiten Projekten bezüglich IT-Sicherheit;
- Beraten von Stellungnahmen (soweit der Aufgabenbereich der EGIS tangiert ist) zu Prüfungen und Anfragen der Rechtsaufsicht, des Bundesrechnungshofes sowie weiterer Prüf- und Kontrolleinrichtungen, die mehrere Rentenversicherungsträger betreffen, und Erarbeiten von Vorschlägen über Konsequenzen aus diesen Prüfungen / Anfragen.

Das **Kontroll- und Steuerungsgremium rvSystem „KS rvSystem“** agiert auf taktischer Ebene und übernimmt aufgabenbezogen im Auftrag der AGIT die Kontroll- und Steuerungsaufgaben der virtuellen Organisation „rvSoftwarehaus“.

Der Begriff rvSoftwarehaus beschreibt die Zusammenführung des virtuellen DRV-IT Softwarehauses mit dem virtuellen Multiprojekt rvEvolution. Auf diese Weise wird für beide Wertschöpfungsnetzwerke (DRV-IT Softwarehaus und rvEvolution) eine effiziente Steuerung von Ressourcen und Mitteln gewährleistet.

DRV-IT Softwarehaus
Die Entwicklung des gemeinsamen Softwaresystems (rvSystem und Beitragsüberwachung) obliegt dem Produktmanagement (PRMJ). Hierzu gehört der gesamte Prozess von der Spezifikation der fachlichen Anforderungen über die Software-Erstellung, den Abnahmetest bis hin zur Software-Bereitstellung. Das PRMJ bildet gemeinsam mit den Subsystemen und den zugeordneten Fach- und Projektgruppen das DRV-IT Softwarehaus.

Die Produktmanager*innen decken insbesondere die originären Aufgaben der gesetzlichen Rentenversicherung sowie Aufgaben, die eng mit diesen verbunden sind, entwicklungstechnisch ab. Zudem werden die funktionalen Schnittstellen zu weiteren IT-Systemen außerhalb des gemeinsamen Softwaresystems koordiniert.

Das PRMJ umfasst folgende Aufgabengebiete:
1. Beitrag;
2. Rehabilitation;
3. Rente;
4. Statistik;
5. eGovernment;
6. Beitragsüberwachung;
7. Ablauforganisation;
8. Technik;
9. Zentrales Management / Releasemanagement.

In die fachlichen Aufgabengebiete (Nummer 1 bis 6 der Aufzählung) fällt die Umsetzung aller Aufgaben, die in Verbindung mit den gesetzlichen Vorschriften für die Rentenversicherung stehen.

Mit dem **Multiprojekt rvEvolution** erfolgt die technische Modernisierung des Softwaresystems rvSystem.

Gremium „Anforderungsmanamgent und Standardisierung“ (AFSTD):
Das Gremium AFSTD ist ebenfalls dem KSrvSystem zugeordnet und hat folgende Aufgaben:

- Identifizierung, Bewertung, Definition und Konsolidierung trägerübergreifender fachlicher Anforderungen (koordiniert mit „Architekturmanagement und Standardisierung“ (ARSTD) und den Fachbereichen) und Entscheidung hinsichtlich

der Umsetzung sowohl für das gemeinsame Softwaresystem als auch für andere gemeinsam in der DRV-IT geplante und genutzte IT-Verfahren;
- Steuerung des zentralen und übergreifenden Anforderungsprozesses der DRV-IT auf der taktischen Ebene;
- Fachlicher Ansprechpartner (Eskalationsinstanz) für die operative Ebene;
- Proaktive Entwicklung fachlicher und organisatorischer Standardisierungen;
- Beratung und Berichterstattung an EGSDIT und Initiierung von Vorlagen für Fachgremien.

Expertengruppe „Steuerung DRV-IT“ (EGSDIT)
Bei der EGSDIT steuert die Projekte, die für die Zusammenarbeit in der DRV-IT wichtig sind, aber nicht unmittelbar das Softwaresystem rvSystem betreffen (zum Beispiel Umstellung der Windows-Versionen, gemeinsames Datennetz, gemeinsame Collaborationsoftware, …).

Darüber hinaus hat sie folgende Aufgaben:
- Erstellen von IT-Rahmenkonzepten und Finanzplanung;
- Prüfung der Wirtschaftlichkeit der eingesetzten IT;
- Erstellen und Nachhalten von IT bezogenen Qualitätsstandards;
- Vorbereiten und Nachhalten von strategischen Entscheidungen zum Weiterentwickeln von ITServices und zur Standardisierung von Hard- und Software.

Gremium Architekturmanagement und Standardisierung“ (ARSTD)
Das Gremium ARSTD, bestehend aus 5 Unternehmensarchitekten der DRV wurde durch die EGSDIT eingesetzt und hat im Schwerpunkt folgende Aufgaben:
- Synchronisierung der Unternehmensarchitektur der DRV-IT mit den strategischen Vorgaben;
- Synchronisierung der Fach- und IT-Architektur;
- Synchronisierung der Informationssystem-, Technologie- und Betriebsarchitektur;
- Synchronisierung der Unternehmensarchitektur der DRV-IT mit den Anforderungen der IT-Sicherheit;
- Steuerung aller Architekturprozesse zwischen allen Beteiligten;
- Erstellung, Pflege und Bereitstellung von Architekturplanungsinformationen;
- Festlegung von Standards und Technologien für die IT-Entwicklung und den IT-Betrieb;
- Beratung von Gremien, Fachgruppen, Trägern und Rechenzentren;
- Verantwortung für die Prüfung der Einhaltung von Vorgaben zur Unternehmensarchitektur der
- DRV-IT und zur Standardisierung (Architektur-Controlling).

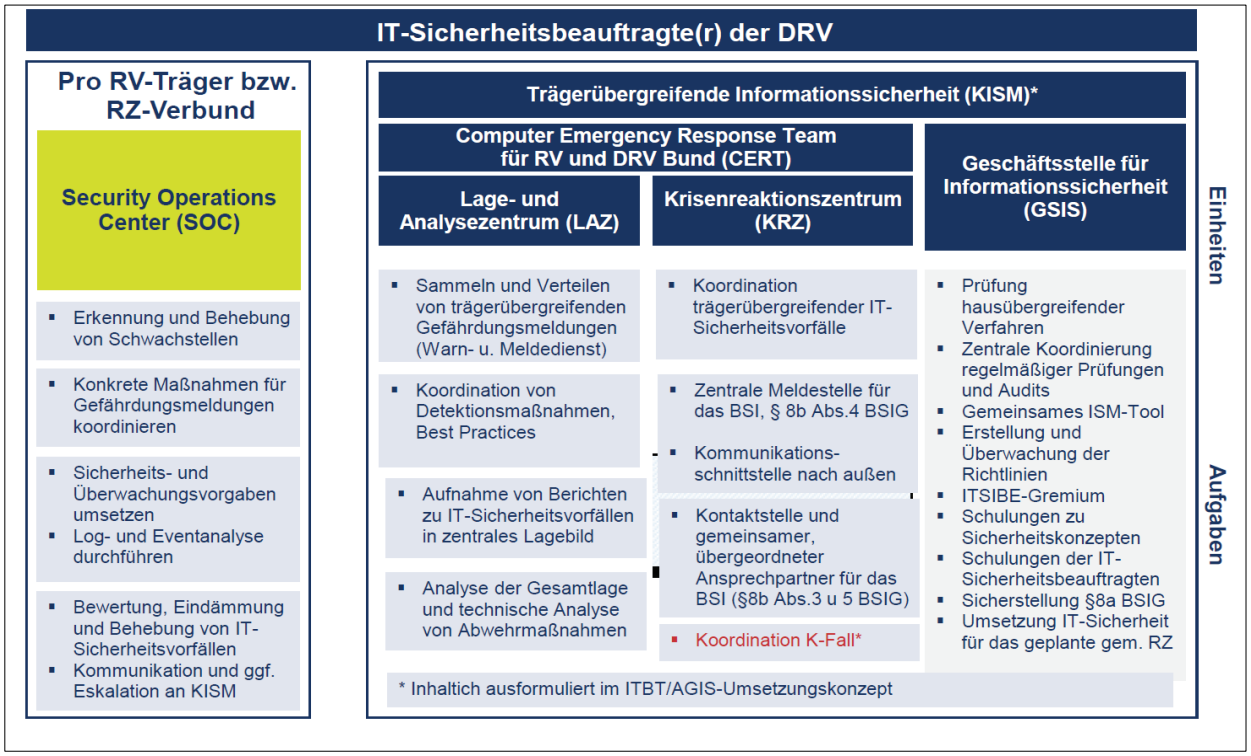
Gremium „IT-Betrieb“ (ITBT)
Die ITBT wurde durch die EGSDIT eingesetzt und hat insbesondere folgende Aufgaben:
- Erarbeiten von Rahmenbedingungen zur Gewährleistung eines reibungslosen und wirtschaftlichen IT-Betriebs durch die Rechenzentren unter Einhaltung der Sicherheitsstandards;
- Analyse und Bewertung des operativen Betriebs aus der Gesamtsicht der DRV-IT auf der Basis von Kennzahlen und Benennung von Maßnahmen zur Verbesserung und Weiterentwicklung;
- Erarbeitung von Rahmenvorgaben zur Vereinheitlichung der IT-Betriebsprozesse und -Infrastruktur in Abstimmung mit dem RZ DRV;
- Definition und Koordination der zwischen den Rechenzentren und Trägern der Deutschen Rentenversicherung abzustimmenden betrieblichen Prozesse und Richtlinien.

Als Steuerungsinstrument für die planmäßige und systematische Weiterentwicklung der Informations- und Kommunikationstechnik in der Deutschen Rentenversicherung dient das jährlich erstellte **IT-Rahmenkonzept**. Es fasst auf der Grundlage der von den Gremien festgelegten IT-Strategie die laufenden beziehungsweise neu aufzusetzenden **IT-Maßnahmen** jahresbezogen zusammen.
Durch die Fest- und Fortschreibung der künftig umzusetzenden Vorhaben im Bereich des IT-Einsatzes, einschließlich der dafür erforderlichen Haushaltsmittel und unter Beachtung daraus resultierender Investitionskosten wird erreicht, dass sowohl die Geschäftsführungen als auch die für den IT-Einsatz verantwortlichen Organisationseinheiten auf verlässliche Basisdaten bei ihren Planungsaktivitäten zurückgreifen können.
Außerdem sorgt das IT-Rahmenkonzept für Transparenz gegenüber den Aufsichtsbehörden und dokumentiert die Zusammenarbeit der Rentenversicherungsträger in der DRV-IT.
Das oberste Entscheidungsgremium in der DRV-IT, der Fachausschuss für Finanzen und Organisation (FAFO) hat im IT-Gesamtplan für 2025 die folgenden strategischen IT-Vorhaben definiert:
• Modernisierung von rvSystem im Rahmen des Programms rvEvolution
• Einführung IPv6 in der Rentenversicherung
• Vorbereitende Maßnahmen zur Einführung von Windows 11 in der DRV

Für diese IT-Vorhaben werden über die zuständigen Gremien die entsprechenden Maßnahmen und Projekte aufgesetzt.
Eine weitere wichtige Rahmenbedingung ist die Verordnung zur Bestimmung „Kritischer Infrastrukturen“ (KRITIS-VO). Als „Kritische Infrastruktur“ wurde auch die Rentenversicherung definiert. Damit sind konkrete Verpflichtungen verbunden. Nach § 8b Absatz 3 BSIG ist innerhalb von sechs Monaten nach Inkrafttreten der KRITIS-VO beim BSI eine Kontaktstelle zu registrieren, um eine jederzeitige Erreichbarkeit sicherzustellen. Nach § 8b Absatz 4 BSIG müssen die Betreiber „Kritischer Infrastrukturen“ erhebliche Störungen ihrer informationstechnischen Systeme und Prozesse an das BSI melden. Ferner muss regelmäßig ein Nachweis erbracht werden, dass organisatorische und technische Vorkehrungen zur Vermeidung von Störungen auf dem aktuellen Stand der Technik getroffen sind.

Vernetzung und Digitalisierung sind wichtige Grundlagen für technologischen Fortschritt. Das E-Government-Gesetz als auch das Online-Zugangsgesetz haben zum Ziel die elektronische Kommunikation mit der Verwaltung zu erleichtern. Die Komplexität der IT sowie die zunehmende Digitalisierung und Vernetzung bieten Cyber-Angreifern aber auch weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Aus dem Blick der Sicherheit von Daten, Prozessen und Kommunikationsverbindungen ist ein wichtiges Ziel, die Risiken beherrschbar zu halten und die Nachteile zu kontrollieren.

Abbildung 2: IT- Sicherheitsbeauftragter der DRV



Als Steuerungsinstrument für die planmäßige und systematische Weiterentwicklung der Informations- und Kommunikationstechnik in der Deutschen Rentenversicherung dient das jährlich erstellte **IT-Rahmenkonzept**. Es fasst auf der Grundlage der von den Gremien festgelegten IT-Strategie die laufenden beziehungsweise neu aufzusetzenden **IT-Maßnahmen** jahresbezogen zusammen.

Durch die Fest- und Fortschreibung der künftig umzusetzenden Vorhaben im Bereich des IT-Einsatzes, einschließlich der dafür erforderlichen Haushaltsmittel und unter Beachtung daraus resultierender Investitionskosten wird erreicht, dass sowohl die Geschäftsführungen als auch die für den IT-Einsatz verantwortlichen Organisationseinheiten auf verlässliche Basisdaten bei ihren Planungsaktivitäten zurückgreifen können.

Außerdem sorgt das IT-Rahmenkonzept für Transparenz gegenüber den Aufsichtsbehörden und dokumentiert die Zusammenarbeit der Rentenversicherungsträger in der DRV-IT.

Das oberste Entscheidungsgremium in der DRV-IT, der Fachausschuss für Finanzen und Organisation (FAFO) hat im IT-Gesamtplan für den Zeitraum 2022-2026 die folgenden vier strategischen IT-Vorhaben definiert:

- Modernisierung von rvSystem im Rahmen des Programms rvEvolution
- Konsolidierung des IT-Betriebs
- Weiterentwicklung der kundenorientierten Online-Services (eGovernment)
- Moderne Formen der Zusammenarbeit

Für diese IT-Vorhaben werden über die zuständigen Gremien die entsprechenden Maßnahmen und Projekte aufgesetzt.

3.3 Rechenzentren

Grundbedingungen für einen akzeptablen Dialogbetrieb sind neben anderen Kriterien nicht zuletzt eine hohe Verfügbarkeit von Antwortzeiten im Bereich von ca. einer Sekunde und ein permanenter und gesicherter Direktzugriff auf alle erforderlichen Daten. Für die Rentenversicherung gilt zum Beispiel, dass selbst das Ergebnis einer kompletten

Rentenberechnung nahezu unmittelbar am Bildschirm angezeigt werden kann und dabei selbstverständlich auch das gesamte Versicherungskonto verarbeitet wird.

Diese zeitlichen Bedingungen müssen aber auch dann gelten, wenn alle angeschlossenen Teilnehmer (von 200 bis zu vielen tausend Anwendern je nach Versicherungsträger) aktiv sind und arbeiten. Zudem müssen alle Informationen grundsätzlich — Einschränkungen bestehen auf Grund datenschutzrechtlicher Bestimmungen — auch an allen Arbeitsplätzen gleichermaßen zur Verfügung stehen. Die dazu erforderlichen Kapazitäten an **Rechenleistung** (CPU-Kapazität), Speicherplatz mit Direktzugriff (**Plattenkapazität**, Speicherkapazität) und Anzahl der anschließbaren Endgeräte stellen in der Rentenversicherung sowohl die Großrechensysteme als auch Systeme der sogenannten mittleren Serverebene sicher.

Diese benötigen aber zunächst schon aus technischen Gründen eine besondere räumliche Umgebung (Raumklima, Temperatur, gleichmäßige Stromversorgung). Die früher erforderliche spezielle Bedienung durch besonders ausgebildete Mitarbeiter (**Operating**), die zudem noch im Schichtdienst arbeiten mussten, wurde weitgehend durch maschinelle Prozesse mit entsprechender Systemunterstützung (Automatisierung der Rechnerüberwachung, Robotersysteme für automatisierte Sicherungen u.a.) abgelöst. Nicht zuletzt stellen auch die datenschutzrechtlichen Bestimmungen (vergleiche Studientext Nummer 32 „Datenschutz in der Rentenversicherung“) Anforderungen an die Sicherheit, die nur in einem zentralen, besonders gesicherten Rechenzentrum erfüllt werden können.

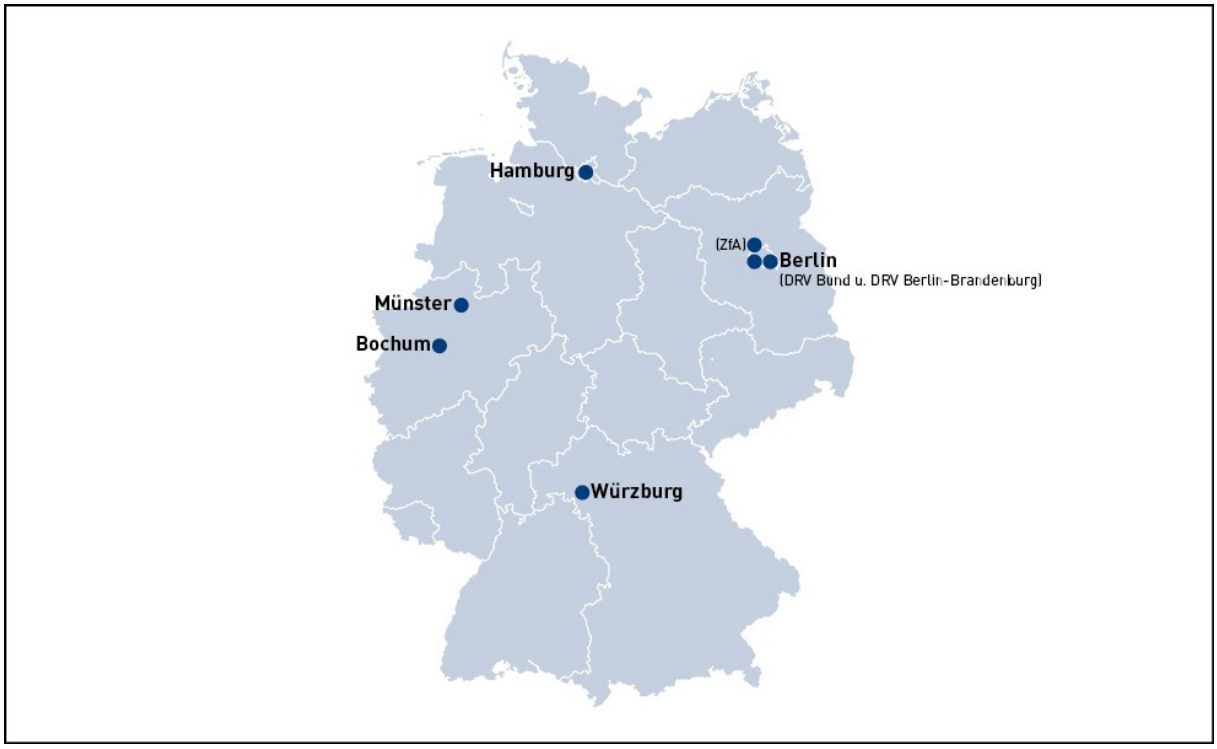
Durch die Vernetzung der einzelnen Rechner und Speichermedien ist zudem ein permanenter Austausch von Informationen, Daten und Anwendungen sichergestellt. Diese Vernetzung kann aber auch gewährleisten, dass bei eventuellen Hardwareausfällen, selbst eines Zentralrechners, dessen Aufgaben zumindest teilweise von anderen Komponenten übernommen werden können (Backup-Prinzip). Denkbar ist dabei auch, dass der Produktivbetrieb der Systeme und die Sicherheit der Daten nicht nur über Inhouse-Komponenten gewährleistet wird, sondern dass ein Backup-Konzept auch in Zusammenarbeit mit einem externen IT-Dienstleister (zum Beispiel Rechenzentrum einer anderen Behörde) auf Gegenseitigkeit organisiert wird. Nach diesem Prinzip arbeiten auch die Träger der Rentenversicherung zusammen, in dem sie sich gegenseitig bei der Datensicherung oder bei Ausfällen von Druckstraßen oder Rechnersystemen unterstützen.

Grundsätzlich unterscheidet die DRV zwei Arten von IT-Dienstleistern. Zum einem werden die gesamtem IT-Dienste (Volldienstleiter), angefangen vom Betrieb der Rechner (Server und Endgeräte) und der darauf ablaufenden Softwarekomponenten und Applikationen, der Infrastruktur (LAN, WAN), der Peripheriesystem (Drucker) und der Programmentwicklung von einem Dienstleister angeboten. Diese umfassenden Dienstleistungen werden beispielsweise von der NOW-IT für ihre Gesellschafter, von der Abteilung 11 der DRV-Bund für ihr Haus und von der IT-Abteilung der KBS erbracht.

Zum anderen gibt es ein so genanntes technisches Infrastruktur-Rechenzentrum (Rechenzentrum Würzburg), das die Netzinfrastruktur, die Großrechner-, die Serversysteme, die Datenhaltungs- und Datensicherungssysteme und die Betriebssysteme und zentrale Dienstleistungen, z.B. in der IT-Sicherheit, für die Kunden bereitstellt. Die auf dieser Infrastruktur ablaufenden Applikationen, angefangen von der systemnahen Software bis hin zu der Implementierung, der Entwicklungsumgebung und den Betrieb von Applikationen wird von den Kunden in enger Zusammenarbeit mit dem Rechenzentrum eigenverantwortlich betrieben. Ebenso unterhalten diese ihre hausbezogene interne Infrastruktur (LAN, Server) und Peripheriesysteme (Drucker).
Die Deutsche Rentenversicherung betreibt seit über 10 Jahren aktiv die Konsolidierung der Rechenzentren, um Synergieeffekte, eine höhere Ausfallsicherheit und letztlich einen wirtschaftlichen IT-Betrieb zu organisieren. Synergieeffekte ergeben sich zum Beispiel durch gemeinsam organisierte Beschaffungen (durch hohe Mengenvolumina wird ein besserer Preis erzielt) oder durch eine größere Arbeitsteiligkeit, wodurch technisches Spezialwissen nicht mehr an jedem Standort vorgehalten werden muss. Hatte noch vor wenigen Jahren

praktisch jeder der Versicherungsträger sein eigenes Rechenzentrum, so ist heute auch bei uns der Zwang zur Konzentration und zu effektiveren Lösungen spürbar.

Abbildung 3: Rechenzentrumsstandorte der Deutschen Rentenversicherung



Gemäß der Entscheidung des Bundesvorstandes der Deutschen Rentenversicherung aus dem Jahr 2019 sind die 16 Rentenversicherungsträger (RV-Träger) dazu verpflichtet, ein Gemeinsames Rechenzentrum zu errichten. Es sind alle Komponenten des Infrastruktur-Betriebs aller Rentenversicherungssysteme (rvSystem) in das RZ-DRV zu überführen. Die Anwendungen von rvSystem sollen auf der Infrastruktur des RZ-DRV auf einer einheitlichen Betriebsplattform betrieben werden. Das RZ-DRV wird an den Standorten Berlin und Würzburg errichtet.
Der Betrieb des RZ-DRV ist eine Aufgabe, die die Rentenversicherung in ihrer Gesamtheit betrifft. Sie dient unter anderem einer engeren Zusammenarbeit im Bereich der Informations- und Kommunikationstechnik.
Auch vor dem Hintergrund permanenter Änderungen im Umfeld der Deutschen Rentenversicherung und damit auch der IT der Deutschen Rentenversicherung (DRV-IT) besteht unter anderem die Notwendigkeit, die Wirtschaftlichkeit der IT-Anwendungen zu verbessern und die zunehmende Bedrohung durch Cyber-Angriffe beherrschbarer zu machen.
Ein besonderes Augenmerk wird dabei auf den effizienten und gleichzeitig sicheren Betrieb der IT-Anwendungen und den besonderen Schutz von Sozialdaten gelegt.
Durch die gemeinsame Verwirklichung dieser Ziele in einem RZ-DRV wird in besonderer Weise die Effizienz der Rentenversicherung gesteigert und der Koordinierungsaufwand zwischen den Trägern verringert. Zudem werden Synergien erschlossen.
Vorstehende Abbildung 3 zeigt den heutigen Stand mit sechs Rechenzentren der Deutschen Rentenversicherung. Erwartete Synergien und der allgemeine Kostendruck machen eine weitere Konsolidierung erforderlich. So mahnt beispielsweise auch der Bundesrechnungshof eine weitere Reduzierung der Rechenzentren aus Kostengründen an.

Derzeit wird im Rahmen eines Projektes am Aufbau eines gemeinsamen Rechenzentrums gearbeitet. Hierfür wurde von der AGIT ein Projektlenkungsausschuss „Gemeinsames Rechenzentrum“ eingesetzt. Dieser ist direkt der AGIT unterstellt (siehe auch Abbildung 1 – Gremienstruktur der DRV-IT).

ZUSAMMENFASSUNG

- In Kapitel 3 ist deutlich geworden, dass die Träger der Rentenversicherung im Bereich der Informationstechnik in der DRV-IT eng zusammenarbeiten, um den Kunden, eine wirtschaftliche, IT von hoher Qualität und entsprechend den IT-Sicherheitsanforderungen anzubieten.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

10. Wie heißen die beiden obersten Entscheidungsgremien in der DRV-IT?

11. In welchen Organisationseinheiten werden die operativen Aufgaben der DRV-IT erledigt?

12. Nennen Sie die Hauptziele des neuen Programmsystems rvDialog.

13. Zählen Sie Gründe auf, warum die Rechenzentren der DRV eng zusammenarbeiten.

14. Warum sind die Datenverbindungen und –netze so wichtig für die DRV?

4. Datenstelle der Rentenversicherung (DSRV)

LERNZIELE

- Sie kennen die Stellung und die Aufgaben der DSRV im Datenaustausch
- Sie wissen, wozu die Stammsatzdatei dient und wie sie genutzt und aktualisiert wird.

Um die rechtliche Stellung und das Konstrukt der Datenstelle der Rentenversicherung (DSRV) besser zu verstehen, ist es hilfreich, sich die Entstehungsgeschichte dieses Bereiches vor Augen zu führen. So entstand Mitte der 1970er Jahre das Bedürfnis zum Austausch von Daten zwischen den verschiedenen Rentenversicherungsträgern. Dazu sollte eine Einrichtung geschaffen werden, welche die Erwerbsverläufe der Versicherten unabhängig vom jeweiligen Versicherungsträger koordiniert.

Anlass war vor allem die Zunahme diskontinuierlicher Erwerbsverläufe und die gestiegene Mobilität der Versicherten, die dazu führten, dass ein Versicherter im Laufe seines Erwerbslebens mitunter bei verschiedenen Regionalträgern oder gar in unterschiedlichen Rentenversicherungszweigen versichert war. Die einzelnen Träger führten daher unter Umständen ein unvollständiges Versicherungskonto, das keineswegs Aufschluss über den gesamten Versicherungsverlauf geben konnte. Damit die bei verschiedenen Trägern vorhandenen Daten eines Versicherten sinnvoll zusammengeführt werden konnten, sollte eine zentrale Datenstelle aller Rentenversicherungsträger beim damaligen Verband Deutscher Rentenversicherungsträger (VDR) aufgebaut werden.

4.1 Rechtliche Stellung der DSRV

Im Jahr 1973 wurde der Arbeitskreis Datenstelle gegründet, der die Grundsätze für die Errichtung der DSRV erarbeitete und 1974 zur Errichtung einer Clearingstelle in Würzburg führte. Die Datenstelle wurde seit ihrer Errichtung vom VDR - seit dem Inkrafttreten der Organisationsreform im Rentenversicherungsrecht zum 01.10.2005 von der Deutschen Rentenversicherung Bund - als funktional verselbständigte Organisationseinheit verwaltet und vom Gesetzgeber mit immer vielfältigeren Aufgaben betraut. Die Rentenversicherungsträger unterhalten nach § 145 Absatz 1 Satz 1 SGB VI gemeinsam eine Datenstelle, die von der Deutschen Rentenversicherung Bund verwaltet wird.

Mit dem sechsten Gesetz zur Änderung des Vierten Buches Sozialgesetzbuch und anderer Gesetze (6. SGB IV-Änderungsgesetz – 6. SGB IV-ÄndG) vom 11. November 2016 wurde die bisherige Bezeichnung der Datenstelle geändert. Diese führt künftig die Bezeichnung „Datenstelle der Rentenversicherung“.

Die DSRV ist das „Eigentum“ sämtlicher Rentenversicherungsträger, das von einer dritten Stelle (der DRV Bund) treuhänderisch verwaltet wird.

Nach § 145 Absatz 1 Sätze 1 und 2 SGB VI ist sicherzustellen, dass die Datenbestände, die die Deutsche Rentenversicherung Bund als Träger der Rentenversicherung führt, und die Datenbestände der Datenstelle der Rentenversicherung dauerhaft getrennt bleiben.

Die Verwaltung der DSRV setzt voraus, dass ihre Angelegenheiten wirtschaftlicher, organisatorischer, technischer und personeller Art von der DRV Bund erledigt beziehungsweise finanziert werden. Dabei ist eine Abhängigkeit von der IT-Organisation der DRV Bund nicht vorgesehen.

Bei der Verwaltung der DSRV handelt es sich nach § 125 Absatz 2 Satz 2 SGB VI um eine gemeinsame Angelegenheit der Träger der Rentenversicherung. Gemeinsame Angelegenheiten sind im Grundsatz- und Querschnittsbereich der DRV Bund zu erledigen und quasi dem Trägerbereich entzogen.

4.2 Aufgaben der Datenstelle

Die DSRV vergibt seit 01.01.2005 zentral für alle Rentenversicherungsträger die Versicherungsnummer und ist alleinige Kommunikationsstelle zwischen diesen und den Stellen außerhalb der Rentenversicherung.

4.2.1 Aufgaben der DSRV als dateiführende Stelle

- Führung der Stammsatzdatei nach § 150 Absatz 1 SGB VI
- Führung der Datei zur Prüfung der A1-Bescheinigungen nach § 150 Absatz 3 SGB VI
- Führung der Basisdatei zur Prüfung bei Arbeitgebern nach § 28p Absatz 8 Satz 2 SGB IV
- Führung der Basisdatei zur Prüfung bei den Zahlungspflichtigen nach § 212a Absatz 5 Satz 3 SGB VI
- Führung der Datei mit Sofortmeldungen nach § 28a Absatz 4 SGB IV und § 150 SGB VI (siehe auch Ziffer 4.2)

4.2.2 Aufgaben der DSRV im Rahmen gesetzlichen Vorgaben

Folgende Aufgaben sind der DSRV im Rahmen gesetzlicher Aufgaben zugeordnet:

- Vergabe von Versicherungsnummern nach § 127 Absatz 1 Satz 1 SGB VI, § 362 SGB V, gegebenenfalls in Verbindung mit §§ 290 Absatz 1 und 291a Absatz 1a SGB V,
- Ausführung des Ausgleichsverfahren nach § 274c Absatz 5 SGB VI (bis 2019),
- Still- und Totlegungen von Versicherungsnummern nach § 3 Absätze 2 und 3 VKVV,
- Durchführung des Kontoführungswechsels nach § 6 VKVV,
- Datenannahme für alle Daten nach § 34 DEÜV,
- Durchführung der Plausibilitätsprüfung nach § 36 Absatz 2 Satz 1 DEÜV,
- Weiterleitung der fehlerfreien Daten an den zuständigen RV-Träger nach § 36 Absatz 2 Satz 2 DEÜV,
- Weiterleitung der fehlerfreien Daten an die Bundesagentur für Arbeit nach § 36 Absatz 3 DEÜV,
- Datenannahme für alle Daten nach §§ 38, 39, 40 und 40a DEÜV und Weiterleitung der fehlerfreien Daten an den zuständigen RV-Träger,
- Funktion zur Registrierung und Authentifizierung für die elektronischen Serviceangebote der RV gem. § 138 Absatz 1 Satz 1 Nummer 10 SGB VI,
- Vermittlungs- beziehungsweise Auskunftsstelle nach § 118 Absatz 3 SGB XII in Verbindung mit §§ 3 Absatz 1 und 11 Absatz 4 SozhiDAV im Zusammenhang mit der Durchführung des Sozialhilfedatenabgleichs,
- Ausstellung von Versicherungsnummernachweisen nach §147 SGB VI (ursprünglich Sozialversicherungsausweise nach § 18h SGB IV),
- Kopf- beziehungsweise Auskunftsstelle nach § 52 Absatz 2a SGB II in Verbindung mit §§ 1 Absatz 2, 1b Absatz 1 und 2 und 2 Absatz 5 GrSiDAV im Zusammenhang mit der Durchführung des Grundsicherungsdatenabgleichs,
- Vermittlungsstelle nach § 37b Absatz 5 WoGG im Zusammenhang mit der Durchführung des Wohngelddatenabgleichs,
- Zugangsstelle für Datenübermittlungen innerhalb der EU nach § 6 Absatz 1 Nummer 3 des Gesetzes zur Koordinierung der Systeme der sozialen Sicherheit in Europa und zur Änderung anderer Gesetze vom 22.06.2011,
- Annahme der Meldungen nach § 5 der 2. Bundesmeldedatenübermittlungsverordnung und Weiterleitung an die Rentenversicherungsträger, Krankenkassen, Bundesagentur und an den Renten Service,
- Datenübermittlung nach § 301 Absatz 1 und 4 SGB V sowie § 302 SGB V,

- Übermittlung der Arbeitgeberdaten im Rahmen der elektronisch unterstützten Betriebsprüfung nach § 28p Absatz 6a SGB IV,
- Datenannahme und -weiterleitung von Meldungen im Rahmen von § 23c SGB IV,
- Datenannahme und -weiterleitung von elektronischen Anträgen im Rahmen von § 151 in Verbindung mit § 150 SGB VI (eAntrag),
- Datenannahme und -weiterleitung der im Versorgungsausgleich erforderlichen Daten im Rahmen von § 229 FamFG,
- Datenannahme und -weiterleitung im Rahmen von § 22a EStG (Rentenbezugsmitteilungen an die ZfA),
- Datenannahme und -weiterleitung im Rahmen von § 32b EStG (Datenaustausch mit der Finanzverwaltung zur Übermittlung der dem Progressionsvorbehalt unterliegenden Leistungen),
- Datenannahme und -weiterleitung im Rahmen des Altersvermögensgesetzes,
- Auskunftserteilung aus der Stammsatzdatei nach §§ 69 ff. SGB X in Verbindung mit § 150 SGB VI,
- Einrichtung von automatisierten Abrufverfahren nach § 79 SGB X in Verbindung mit §§ 148 Absatz 3, 150 SGB VI,
- Datenabgleich mit der Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG) nach § 73 Absatz 2 Gesetz über die Alterssicherung der Landwirte – ALG –,
- Elektronische Anforderung von Bescheinigungen vom Arbeitgeber zur Berechnung von Übergangsgeld nach § 23c Absatz 2 Satz 2 und 3 SGB IV,
- Elektronische Übermittlung von Bescheinigungen vom Arbeitgeber an die Träger der Rentenversicherung nach § 196a SGB VI in Verbindung mit § 23c Absatz 2b SGB IV (Bescheinigungen elektronisch anfordern und annehmen - rvBEA),
- Elektronische Anforderung der „Gesonderten Meldung“ beim Arbeitgeber nach § 194 Absatz 1 SGB VI,
- Versicherungsnummern-Abfrageverfahren für Arbeitgeber § 28a Absatz 3a SGB IV,
- Verarbeitung der Identifikationsnummern nach §11 RentÜG

4.2.3 Aufgaben der DSRV aufgrund Einschaltung als Vermittlungsstelle durch die Rentenversicherungsträger

Die DSRV kann nach § 145 Absatz 1 Satz 3 SGB VI von den RV-Trägern als Vermittlungsstelle eingeschaltet werden. Dies ist in folgenden Verfahren geschehen:

- Übermittlung von Zahldaten der Träger der allgemeinen Rentenversicherung an den Renten Service
- Vereinbarung über das maschinell unterstützte KVdR-Meldeverfahren nach § 201 SGB V Vergabe einer Versicherungsnummer als Zulagennummer im Zulageverfahren Pflegeversicherung
- Datenannahme und -weiterleitung der im Erstattungsverfahren erforderlichen Daten im Rahmen vom §103 SGB X

4.2.4 Aufgaben der DSRV aufgrund vertraglicher Regelungen (zum Beispiel: § 80 SGB X / § 11 BDSG) mit Rentenversicherungsträgern

- Bereitstellung von Online-Dienstleistungen im Internet nach § 80 SGB X
- Abrechnung von Reisekosten für Rehabilitanden im Verfahren „Maschineller Reisekostengutschein“ nach § 80 SGB X
- Annahme, Versand und Weiterleitung von De-Mails nach dem De-Mail-Gesetz (wurde Mitte 2025 eingestellt)
- Betrieb von Fachverfahren im Auftrag der Rentenversicherungsträger
- Pflege und Bereitstellung der Beitragssatzdatei der Krankenkassen für die Rentenversicherungsträger
- Pflege und Bereitstellung der Devisenkursdatei für die Rentenversicherungsträger

Beispiele:

Übermittlung des Datums der letzten Eheschließung oder der Begründung einer Lebenspartnerschaft aus den Daten der Meldebehörden nach § 5 Absatz 1 Nummer 9 der 2. BMeldDÜV in Verbindung mit § 196 Absatz 2a SGB VI im Auftrag der Rentenversicherungsträger an den Renten Service der Deutschen Post AG, um schneller Zahlungen von Hinterbliebenenrenten an Berechtigte einstellen zu können.

Bereitstellung des Dienstes „Auskünfte Gerichtsvollzieher“ – Im Auftrag der Rentenversicherungsträger teilt die Datenstelle auf elektronische Anfrage den Gerichtsvollziehern aktuelle Anschriften Betroffener oder Namen und Anschriften von Arbeitgebern mit (§ 74 Absatz 2 SGB X – eGerichtsvollzieher).

Verfahren eTermin – Im Auftrag der Rentenversicherungsträger verwaltet die Datenstelle eine Datei, in der Versicherte oder andere Interessenten über das Internet eine online Terminvergabe für eine Auskunfts- und Beratungsstelle vereinbaren können.

4.2.5 Aufgaben der DSRV aufgrund vertraglicher Regelungen mit Sozialversicherungsträgern

Die Behörden der Zollverwaltung und die sie gemäß § 2 Absatz 2 unterstützenden Stellen sind verpflichtet, einander die für deren Prüfungen erforderlichen Informationen einschließlich personenbezogener Daten und die Ergebnisse der Prüfungen zu übermitteln, soweit deren Kenntnis für die Erfüllung der Aufgaben der Behörden oder Stellen erforderlich ist. (§ 6 Absatz 1 Satz 1 SchwarzArbG)

In der Zusammenarbeitsvereinbarung zwischen der Finanzkontrolle Schwarzarbeit (FKS) und der DRV wird die DSRV beauftragt, die Infrastruktur für den Datenaustausch zwischen dem Zoll und den Trägern der Rentenversicherung bereitzustellen.

4.3 Der Stammsatzbestand

Die Versicherungsnummer (VSNR) ist der zentrale Ordnungsbegriff (siehe auch Kapitel 5) in der Deutschen Rentenversicherung. Jeder Versicherte der gesetzlichen Rentenversicherung erhält eine Versicherungsnummer; sie begleitet ihn ein ganzes Leben lang. Unter diesem Kennzeichen speichert der zuständige Rentenversicherungsträger alle wichtigen Daten in einem Versicherungskonto.

Zu jeder Versicherungsnummer wird bei der DSRV ein Stammsatz eingerichtet, der neben

- der Versicherungsnummer, und bei Beziehern einer Rente wegen Todes auch die Versicherungsnummer des verstorbenen Versicherten,
- den Familiennamen, Vornamen einschließlich des Geburtsnamens,
- den Geburtsort einschließlich des Geburtslandes,
- die Staatsangehörigkeit,
- Sterbedatum,
- die Anschrift,
- Betriebsnummer des Arbeitgebers
- Tag der Beschäftigungsaufnahme

sowie weitere technische Informationen enthält.

Die Stammsatzdatei gewährleistet, dass eine rentenversicherte Person nur eine Versicherungsnummer erhält und eine vergebene Versicherungsnummer nicht noch einmal für eine andere Person verwendet wird. Außerdem kann mit ihr durch Vergleich der persönlichen Merkmale eine vorhandene Versicherungsnummer festgestellt werden. Hierzu werden auch Verfahren genutzt (Phonetik), mit denen unterschiedliche Schreibweisen von Namen und Adressen erkannt und auf einen Wortstamm zurückgeführt werden können.

Eine weitere Funktion des Stammsatzes ist es, zu erkennen welcher der Rentenversicherungsträger zuständig ist. Dies wird bei jeder Weiterleitung von Daten an den aktuellen Kontoführer benötigt.

Die nachstehende Tabelle zeigt den Gesamtbestand dieser vergebenen Versicherungsnummern zum 1. Januar 2026 untergliedert nach einigen wichtigen Fallgruppen (zu den still- beziehungsweise totgelegten Versicherungsnummern siehe Kapitel 5):

Tabelle 1: Stammsatzbestand am 1.1.2026

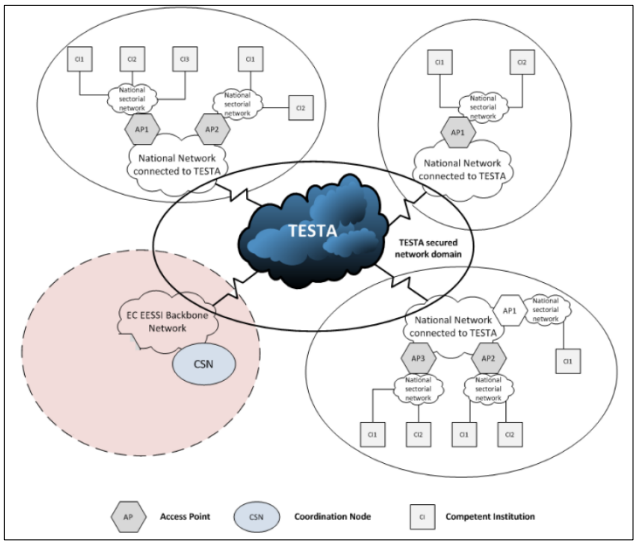
Fallgruppe	**Anzahl**
Gesamtbestand	**163.114.771**
- Stillgelegte VSNR	10.538.069
- Totgelegte VSNR	767.298
- Aktive VSNR	151.386.534
- Gestorbene Versicherte	42.942.066
- Lebende Versicherte	120.172.705
- Versichertenrentner	20.997.932
- Reine KLG-Empfänger	560
Aktiv Versicherte	**87.453.454**
- davon Ausländer	29.179.106

4.4 EU-weite Kommunikation der Sozialversicherung im Rahmen des Verfahrens EESSI

EESSI (Electronic Exchange of Social Security Information) ist ein IT-System, das den Sozialversicherungsträgern gemäß den EU-Vorschriften zur Koordinierung der Systeme der sozialen Sicherheit EU-weit einen schnelleren und sichereren Informationsaustausch über geltende Rechtsvorschriften und Aspekte wie Krankheit, Berufskrankheit und Arbeitsunfälle, Rente, Arbeitslosigkeit und Familienleistungen ermöglicht. Zuvor erfolgte der Austausch vorwiegend auf Papier. Mit der Einführung von EESSI wurde zunehmend auf elektronischen Informationsaustausch umgestellt. Der Datenaustausch erfolgt über 99 definierte Anwendungsfälle (Business Use Cases / BUCs), mit hierzu festgelegten Datensätzen (sog. Structured Electronic Documents / SEDs).

In Abbildung 4 wird die Gesamtarchitektur dargestellt.

Abbildung 4: EESSI Gesamtarchitektur



➔ Aktuell gibt es 51 Access Points (APs) in 32 Ländern, die den Nachrichtenaustausch zwischen Staaten beziehungsweise einzelnen Sektoren in den Staaten wie dem Rentensektor abwickeln.
➔ An die APs sind die verschiedenen IT-Systeme der nationalen Anwendungen angebunden.
➔ Derzeit sind über 3370 Trägerinstitutionen (Competent Institutions) durch das System verbunden, die in einem zentralen Verzeichnis samt ihrer Zuständigkeiten / Kompetenzen hinterlegt sind (Central Service Node / CSN).

Quelle: EESSI – Certificate Management Guide S. 5

Der Access Point APDE02 wird bei der DSRV betrieben und dient als Schnittstelle zum Ausland. Daran angebunden sind die Träger der Rentenversicherung, das A1-Annahmeverfahren für die bei der DSRV geführten A1-Datenbank sowie die Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V. (ABV), die Generalzolldirektion (GZD) und die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG).

Die Deutsche Rentenversicherung setzt für EESSI auf die Nutzung ihrer nationalen Anwendung rvSystem, welche hierfür modular erweitert wurde. Die Kommunikation innerhalb der DRV besteht im Wesentlichen aus folgenden Komponenten beziehungsweise zeichnet sich durch folgende Merkmale aus:

- Das National Gateway ist die zentrale Komponente bei der DSRV, die folgende Aufgaben übernimmt:
- Ermittlung des zuständigen Rentenversicherungsträgers anhand von Daten aus dem SED (Datensatz) und einer nationalen Datenbank
- Automatisierte Verarbeitung von Nachrichten, bei denen eine Mitwirkung der Sachbearbeitung nicht notwendig ist.
- Automatisierter Versand von Nachrichten zur Mitteilung einer geltenden Rechtsvorschrift bei Entsendungen von Arbeitnehmern ins EU-Ausland
- Die SEDs werden dann über Standardverfahren der deutschen Rentenversicherung (Objektbasierter Datenaustausch der Rentenversicherung / ODRV) an die RV-Träger übermittelt.
- Einige Daten aus den SEDs werden in die Konten der Versicherten übernommen.
- Das SED wird dem Sachbearbeiter als pdf im rvPUR (Postkorb- und Rechercheclient) dargestellt.
- Die Oberflächen der Sachbearbeitung zur Bearbeitung von Antragsformularen wurden um die europäischen Sachverhalte ergänzt.

Ziel war und ist, einen hohen Automatisierungsgrad herzustellen, also umfassend nationale Anwendungen an EESSI anzubinden.

Die Deutsche Rentenversicherung ist seit Juni 2020 mit allen ihr zugewiesenen Geschäftsprozessen im EESSI-System in Produktion. Seitdem erfolgt der elektronische Nachrichtenaustausch mit allen bereitstehenden Partnern im EU-Ausland via EESSI. Bereits im Juli 2019 hatte der Austausch in EESSI begonnen, zunächst mit Geschäftsprozessen, die keine Sachbearbeitungsinteraktion benötigen (A1-Datenbank).

Die Länder, mit denen der umfangreichste EESSI-Nachrichtenaustausch über den Access Point der DSRV stattfindet, sind Polen, Österreich, Italien, Frankreich, die Niederlande, Belgien und Spanien.

Monatlich (Stand: November 2025) werden ca. 185.000 Nachrichten von den RV-Trägern in Richtung EU-Ausland und umgekehrt ca. 240.000 Nachrichten ausgetauscht.

4.5 Kommunikationspartner zu verschiedenen Stellen innerhalb und außerhalb der Sozialversicherung

Die DSRV ist nicht nur ein verlässlicher Kommunikationspartner zu Trägern der Deutschen Rentenversicherung oder anderen Sozialversicherungsträgern, sondern unterhält unter anderem auch Datenverbindungen zur Justiz, Arbeitgebern, Kommunen oder zum Zoll.
Die DSRV verarbeitet jährlich etwa 2 Milliarden Datensätze.

Abbildung 5: Die DSRV als Kommunikationspartner

ZUSAMMENFASSUNG

Kapitel 4 zeigte die zentrale Stellung der Datenstelle der Rentenversicherung im Kommunikationsprozess innerhalb der Rentenversicherung und mit externen Stellen.
Der bei der DSRV geführte Stammsatzbestand gewährleistet dabei die Eindeutigkeit des Ordnungsbegriffs Versicherungsnummer und dient der Ermittlung des jeweils aktuell zuständigen Versicherungsträgers.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

15. Nennen Sie die gesetzlichen Grundlagen für die Unterhaltung der DSRV und deren Aufgaben?

16. Durch welche Datei sollen Mehrfachvergaben ausgeschlossen werden?

17. Wie viele Versicherungsnummern wurden bislang vergeben? Wie viele ausländische Versicherte werden derzeit gezählt?

18. Nennen Sie beispielhaft einige wesentliche Aufgaben der DSRV.

5. Versicherungsnummer als Ordnungsbegriff

LERNZIELE

- Sie kennen die Rechtsgrundlage der Versicherungsnummer.
- Sie können den Sinn, den Aufbau sowie das Vergabeverfahren der Versicherungsnummer erklären.
- Sie wissen, warum die Versicherungsnummer bei der Erstellung einer Krankenversicherungsnummer benötigt wird.

Sie haben bereits gesehen, dass im Rentenversicherungssystem das Versicherungskonto von immenser Bedeutung ist und welche Vielzahl an Daten erforderlich ist, um die Aufgaben eines Rentenversicherungsträgers abdecken zu können. Damit alle Leistungen und Auskünfte zu einem Versicherten aus dem Versicherungskonto berechnet und ermittelt werden können, ist es erforderlich, dass alle Daten, die dem Versicherten zugeordnet sind, auch in dessen Versicherungskonto zentral zusammengeführt sind. Um dies gewährleisten zu können, wurde der eindeutige Ordnungsbegriff der „Versicherungsnummer“ eingeführt. Wir wissen bereits aus dem vorherigen Kapitel, dass es eine der Hauptaufgaben der DSRV ist, die Eindeutigkeit der Zuordnung von Versicherungsnummer zu Versicherten sicher zu stellen.

5.1 Rechtliche Grundlagen, Sinn und Aufbau der Versicherungsnummer

Rechtsgrundlage für die Versicherungsnummer

Nach § 149 Absatz 1 Satz 1 SGB VI ist die Versicherungsnummer zwingend das datentechnische Ordnungskriterium für die Versicherungskonten, da diese „*nach der Versicherungsnummer geordnet“* sind.

Aus § 147 Absatz 1 SGB VI folgt, dass die Vergabe einer Versicherungsnummer für alle nach dem SGB VI geführten Versicherungskonten zwingend vorgeschrieben ist.

In § 147 Absatz 2 SGB VI sind die - teilweise personenbezogenen - Merkmale aufgezählt, aus denen sich die Versicherungsnummer zusammensetzt. Das Verfahren zur zentralen Vergabe einer Versicherungsnummer soll sicherstellen, dass jede Versicherungsnummer nur einmal vergeben wird und jeder Versicherte auch nur eine Versicherungsnummer erhält.

Zweck der Versicherungsnummer

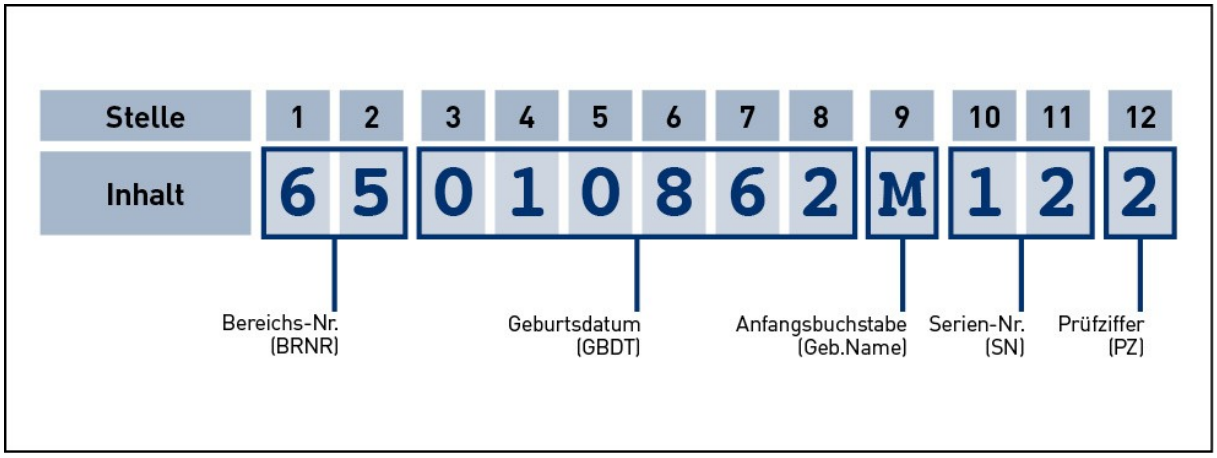
Die Versicherungsnummer ist damit ein für die gesamte gesetzliche Rentenversicherung eindeutiger und einheitlich gültiger Ordnungsbegriff. Die Daten jeder einzelner Versicherten lassen sich damit unverwechselbar kennzeichnen und von den Daten jedes anderen Versicherten eindeutig unterscheiden. Nachdem die Versicherungsnummer als Ordnungsbegriff für die Führung der Versicherungskonten verwendet wird, stellt sie die Eindeutigkeit auch für die Versicherungskonten sicher.

Auch das Meldeverfahren nach der DEÜV basiert auf der Verwendung der Versicherungsnummer. Nach diesen Bestimmungen ist bei allen Meldungen die Versicherungsnummer zur Zuordnung zu verwenden, wenn personenbezogene Daten übermittelt werden. So ist sichergestellt, dass alle Daten maschinell, ohne aufwändige manuelle Bearbeitung, in die korrekten Versicherungskonten übernommen werden können.

Aufbau der Versicherungsnummer

Die Versicherungsnummer muss eindeutig sein. Ihre Zusammensetzung ist daher in § 147 Absatz 2 SGB VI geregelt. Das heißt, die Versicherungsnummer muss die nachfolgend aufgeführten Merkmale aufweisen, darf aber keine weiteren personenbezogenen Merkmale enthalten (vergleiche Abbildung 6 **Fehler! Verweisquelle konnte nicht gefunden werden.**). Die Versicherungsnummer umfasst 12 Stellen und setzt sich aus insgesamt fünf Merkmalen zusammen (vergleiche hierzu auch den Studientext Nummer 3 „Beitrags- und Meldeverfahren“).

Abbildung 6: Aufbau einer Versicherungsnummer



5.2 Vergabe der Versicherungsnummer

Jede Versicherungsnummer wird zentral durch die Datenstelle der Rentenversicherung (DSRV) vergeben (§ 147 SGB VI i. V. m § 1 Absatz1 der Versicherungsnummern-, Kontoführungs- und Versicherungsverlaufsverordnung – VKVV).

Das zum 01.01.2005 in Kraft getretene Gesetz zur Organisationsreform in der gesetzlichen Rentenversicherung (RVOrgG) hatte eine neue Versichertenverteilung zur Stabilisierung der Arbeitsmengen bei den Rentenversicherungsträgern zum Ziel. Die Unterscheidung zwischen Arbeitern und Angestellten wurde aufgegeben. Die Versicherten werden seit 2005 im Zuge der Vergabe der Versicherungsnummer unabhängig von ihrer tatsächlich ausgeübten Tätigkeit entsprechend einer im Gesetz festgelegten Quote einem Rentenversicherungsträger zugeordnet. Die Versicherungsnummer kann wegen dieser versicherungsträgerübergreifenden Quotierung nicht mehr durch die Rentenversicherungsträger selbst vergeben werden, wie dies bis 2005 der Fall war.

Eine einmal fehlerfrei vergebene Versicherungsnummer behält der Versicherte während seines gesamten Lebens (§ 3 Absatz 1 VKVV), auch wenn er zum Beispiel wegen Heirat seinen Namen ändert. Selbst nach seinem Tode wird sie gegebenenfalls noch für die Bewilligung und Zahlung von Hinterbliebenenrenten verwendet und daher nicht gelöscht.

Mögliche Anlässe für die Vergabe einer Versicherungsnummer sind:

- die Aufnahme einer Beschäftigung,
- der Bezug von Leistungen einer Krankenkasse oder der Bundesagentur für Arbeit, für die Beiträge zu entrichten sind,
- eine Geburtsanzeige durch die Meldebehörden (für die Anerkennung von Kindererziehungszeiten bei den Eltern)

  sowie

- ein Kontenklärungs-, Auskunfts-, Leistungs- oder Beitragsentrichtungsantrag bei einem Rentenversicherungsträger

Versicherungsnummernachweis

Bis 2023 wurde durch die Datenstelle der Rentenversicherung bei der Vergabe einer Versicherungsnummer ein Sozialversicherungsausweis nach § 18h SGB IV ausgestellt. Da ein Sozialversicherungsausweis schon seit vielen Jahren nicht mehr ausgestellt, sondern den Versicherten lediglich ein Nachweis über die Versicherungsnummer übermittelt wird, wurde die bisherige Praxis gesetzlich geregelt und das Dokument in Versicherungsnummernachweis umbenannt.

Die Regelung zur Information der Versicherten über die Versicherungsnummer in Form eines Versicherungsnummernnachweises wurde in § 147 SGB VI zusammengefasst. Der neue Nachweis wird weiterhin für die Personen ausgestellt, an die die Datenstelle der Rentenversicherung eine Versicherungsnummer vergeben hat, und enthält nur folgende Daten - Versicherungsnummer, den Familien- und Geburtsnamen sowie die Vornamen und Ausstellungsdatum.

5.3 Vergabeverfahren

Die **Verteilung der Versicherten auf die Träger der Rentenversicherung im Vergabeverfahren** ist wie folgt geregelt:

Deutsche Rentenversicherung Knappschaft-Bahn-See (DRV KBS)

Versicherungsnummern werden an die Deutsche Rentenversicherung Knappschaft-Bahn-See nach § 127 Absatz 2 Nummer 1 SGB VI im Umfang von 5 % zugeordnet. Primär werden dabei die Versicherten der in §§ 129 und 133 SGB VI festgelegten Branchen berücksichtigt.

Da allein mit diesen Fällen die Quote von 5 % nicht erreicht wird, werden der Deutschen Rentenversicherung Knappschaft-Bahn-See über diesen Personenkreis hinaus noch weitere Fälle zugeordnet. Dabei werden nur Versicherte in Brandenburg, Hamburg, Hessen, Nordrhein-Westfalen, Oberbayern, Sachsen und im Saarland berücksichtigt und gleichmäßig zugewiesen.

Deutsche Rentenversicherung Bund (DRV Bund)

Der Deutsche Rentenversicherung Bund werden 40 % der zu vergebenden Versicherungsnummern gemäß § 127 Absatz 2 Nummer 1 SGB VI zugeordnet.

Regionalträger

Den Regionalträgern werden 55 % der zu vergebenden Versicherungsnummern zugeordnet. Innerhalb der Regionalträger wird gemäß § 127 Absatz 2 Nummer 3 SGB VI die Versicherungsnummer nach regionaler Zuständigkeit des Versicherungsträgers zugeordnet.

Technische Realisierung

Bei der Vergabe einer Versicherungsnummer ist zunächst die maßgebliche Regionalnummer (Stelle 1 und 2 der Versicherungsnummer) primär aus dem Wohnort beziehungsweise Aufenthaltsort des Versicherten zu ermitteln. Die Nummer entspricht den Bereichsnummern der Regionalträger von 02 bis 29 (vergleiche Anlage zur VKVV). Bei Wohnsitz im Ausland ist die Regionalnummer der nach über- und zwischenstaatlichem Recht zuständigen Verbindungsstelle für den Wohnsitzstaat maßgeblich (zum Beispiel bei Wohnsitz in Italien die Regionalnummer der DRV Schwaben [21]).

Nach Festlegung der Regionalnummer wird zur korrekten Verteilung der Versicherten entsprechend der Quoten ein dreistufiges Verfahren durchlaufen:

- **Phase 1:** Versicherte werden vorab gemäß § 129 oder § 133 SGB VI der DRV KBS zugeordnet und auf deren Quote von 5 % angerechnet.

- **Phase 2:** Zuordnung der verbleibenden Versicherten zu den Regionalträgern, so dass für jeden örtlichen Zuständigkeitsbereich eines Regionalträgers gesondert jeweils die Quote von 55 % erreicht wird. Innerhalb der Regionalträger wird für die Versichertenzuweisung wie bisher vor allem auf den Wohnort beziehungsweise Aufenthaltsort abgestellt.

- **Phase 3:** Verteilung der übrigen Versicherten auf Bundesebene, so dass die DRV Bund im Ergebnis 40 % und die DRV KBS 5 % der Gesamtversicherten erhalten. Dabei werden bei der DRV KBS die bereits nach dem ersten Schritt zugeordneten Versicherten auf die Quote angerechnet und ihr nur Versicherte in den Regionen Brandenburg, Hamburg, Hessen, Nordrhein-Westfalen, Oberbayern, Sachsen und im Saarland gleichmäßig zugewiesen.

Die Vergabe der Versicherungsnummer erfolgt vollmaschinell, ohne manuelle Eingriffe der Sachbearbeitung. Lediglich in den Fällen, in denen bei der DSRV die maschinelle Identitätsprüfung kein eindeutiges Ergebnis liefert (Verdacht auf eine Mehrfachvergabe), muss die Sachbearbeitung aufklärend eingreifen.

Über die Vergabe einer Versicherungsnummer wird die versicherte Person schriftlich informiert, in der Regel wird auch ein Versicherungsnummernachweis (ursprünglich Sozialversicherungsausweis) zugestellt. Außerdem erhält der zuständig gewordene Rentenversicherungsträger die Aufforderung zum Aufbau eines Versicherungskontos (siehe auch Kapitel 6) und bei Bedarf wird die Stelle informiert, die ausschlaggebend für die Vergabe war (zum Beispiel Arbeitgeber oder Krankenkasse bei Beschäftigungsaufnahme).

Mehrfach- und Doppelvergabe

Eine Versicherungsnummer wird nicht berichtigt, selbst wenn sich der Name ändert oder ein anderer Versicherungsträger zuständig wird.

Stellt sich jedoch heraus, dass trotz der vorher aufgezeigten Mechanismen in Einzelfällen an einer Versicherten mehrere Versicherungsnummern vergeben wurden (**Mehrfachvergabe**) oder dass eine Versicherungsnummer fehlerhaft ist, so ist sie zu sperren (**Stilllegung**).

Fehlerhaft ist eine Versicherungsnummer, wenn entweder das Geburtsdatum oder die Seriennummer hinsichtlich der Geschlechtsspezifikation unzutreffend ist. Bei einer Stilllegung bleiben sowohl das Versicherungskonto als auch der Stammsatz dem Grunde nach bestehen.

Sie werden lediglich als stillgelegt gekennzeichnet und ein Verweis auf die zutreffende Versicherungsnummer aufgenommen. Eventuelle Daten aus dem stillgelegten Konto werden in das aktuelle Konto übertragen. Die Stilllegung erfolgt in gleicher Weise wie die Vergabe, nämlich über ein Datenaustauschverfahren. Im Gegensatz zur Versicherungsnummernvergabe ist hier jedoch die Sachbearbeitung sowohl sachaufklärend als auch auslösend an der Stilllegung beteiligt.

Stellt sich heraus, dass dieselbe Versicherungsnummer an verschiedene Versicherte vergeben worden ist, muss die Versicherungsnummer nach § 3 Absatz 3 VKVV **tot gelegt** werden. Die Versicherten erhalten jeweils eine neue Versicherungsnummer. Eine Verbindung der aktuellen Versicherungsnummer zur tot gelegten besteht bei diesen **Doppelvergaben** im Gegensatz zur Stilllegung nicht.

5.4 Versicherungsnummer als Basis der Krankenversichertennummer

Die gesetzlichen Krankenkassen sind seit 01.01.2004 nach § 290 SGB V verpflichtet, für ihre Verfahren eine eindeutige Krankenversichertennummer (KVNR) zu nutzen. Die Vergabe ist durch Richtlinien zu regeln.

Die Spitzenverbände der Krankenversicherung hatten sich auf dieser Basis im Jahr 2004 an die Rentenversicherung gewandt und um Unterstützung bei der Einführung einer eigenständigen KVNR gebeten. Dabei sollten insbesondere Verfahrens- und um kostenspezifische Sachverhalte betrachtet werden. Die unmittelbare Verwendung der Versicherungsnummer hatte der Bundesbeauftragte für den Datenschutz unmissverständlich abgelehnt.

Die mit dem BMGS abgestimmten Richtlinien zur Krankenversicherungsnummer (KVNR) sehen einen zehnstelligen Ordnungsbegriff vor, der als Pseudonym aus der Rentenversicherungsnummer (VSNR) ermittelt wird. Die Krankenversichertennummer umfasst grundsätzlich 20 Stellen. Sie besteht aus

- dem unveränderbaren Teil (zehnstelligem Pseudonym aus der Versicherungsnummer),
- der bundeseinheitlichen Angabe zur Kassenzugehörigkeit (das neunstellige Institutionskennzeichen der Krankenkasse)

  und

- einer Prüfziffer.

Hinzu kommt krankenkassenintern eine Erweiterung um bis zu 10 Stellen zur Kennzeichnung der Zusammengehörigkeit von mitversicherten Familienangehörigen mit einem Mitglied.

Unter Pseudonymisierung versteht man dabei eine Einwegverschlüsselung, die keine Rückschlüsse auf die ursprüngliche Versicherungsnummer zulässt, aber angewandt auf die gleiche Versicherungsnummer stets das gleiche Pseudonym erzeugt. Jede Krankenkasse ermittelt über ein Auskunftsverfahren die Versicherungsnummer für ihre Versicherten. Die Vertrauensstelle der Krankenversicherung nimmt die von den Krankenkassen gemeldete Versicherungsnummer eines Versicherten an und prüft, ob zu ihr bereits ein Pseudonym vorliegt, andernfalls erzeugt sie ein neues Pseudonym. Sie führt ein Verzeichnis aller zu den

Versicherungsnummern vergebenen Pseudonyme, um eine Dublettenvergabe zu vermeiden. Insofern wird die Doppelvergabe durch die Schutzmechanismen der Rentenversicherung verhindert. Personenidentifizierende Stammdaten eines Versicherten werden von der Vertrauensstelle nicht benötigt. Im Zuge des KVNR-Vergabeverfahrens werden die neu vergebenen Versicherungsnummern nach den allgemeinen Verteilregeln innerhalb der Rentenversicherung auf die Versicherungsträger aufgeteilt. Durch die Vergabe an weitere Personen, für die bisher in der Rentenversicherung kein Konto geführt wird, entstehen im Rahmen der Versichertenverteilung nach § 127 SGB VI zusätzliche Versicherungskonten; Versicherungszeiten werden zunächst nicht gemeldet.

Seit 01.07.2022 werden die Versicherungsnummern auch für Versicherte der privaten Krankenversicherungen und seit 01.01.2025 für die Heilfürsorgeberechtigten der Bundespolizei nach § 290 SGB V in Verbindung mit § 362 SGB V vergeben. Diese Versicherungsnummer dient bei den Unternehmen der privaten Krankenversicherung und bei der Bundespolizei als Basis für die Ausstellung einer elektronischen Gesundheitskarte beziehungsweise elektronischen Identität, welche die Grundlage für die Nutzung der digitalen Angebote im Gesundheitswesen darstellt.

Nachdem auch für die Versicherten der privaten Krankenversicherung eine PVNR auf der Basis der Versicherungsnummer der Rentenversicherung vergeben wird, haben nahezu alle Teile der Bevölkerung in der Bundesrepublik eine VSNR erhalten. Versicherungsnummern, die als Basis der KVNR oder PVNR neu vergeben wurden, waren bis 2024 noch „inaktiv“, da bislang keine rentenrechtlichen Sachverhalte (zum Beispiel Beschäftigungsaufnahme) existierten. Bei den Vergaben einer Versicherungsnummer im Rahmen der Vergabe einer KVNR oder PVNR an zusätzliche Personen, die nicht der Rentenversicherung angehören, wurde auch kein Versicherungsnummernachweis (ursprünglich Sozialversicherungsausweis) ausgestellt, weil dieser meistens gar nicht oder erst Jahre später gebraucht wird. Erst mit Eintritt von einem der in Kapitel 5.2 genannten Vergabegründe wurde eine solche bislang ruhende Versicherungsnummer aktiviert.

Seit 2024 wurde die Verfahrensweise geändert und die ursprüngliche Aktivierung der Versicherungsnummer ist weggefallen. Alle Versicherungsnummern werden jetzt als aktive Versicherungsnummern vergeben. Auch der Versicherungsnummernachweis (urspr. Sozialversicherungsausweis) wird direkt ausgestellt.

ZUSAMMENFASSUNG

- In Kapitel 5 haben wir gesehen, welche Bedeutung der Versicherungsnummer als zentralem Ordnungsbegriff für die Rentenversicherung zukommt.

  Wir haben ferner die Rolle der Versicherungsnummer bei der Vergabe der Krankenversicherungsnummer kennen gelernt.

  Außerdem wurde gezeigt, nach welchen Richtlinien die Versicherungsnummernvergabe erfolgt und wie dieses Verfahren technisch bei der DSRV abläuft.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

19. Welche Bestimmung schreibt die Verwendung der Versicherungsnummer als Ordnungskriterium vor? Welche Bestimmung beschreibt den Inhalt der Versicherungsnummer?

20. Was ist der Sinn der Versicherungsnummer?

21. Nennen Sie die Merkmale der Versicherungsnummer.

22. Welches Merkmal wird bei der Vergabe der Versicherungsnummer zuerst festgelegt?

23. Welcher Stelle der Rentenversicherung kommt im Rahmen der Vergabe eine zentrale Funktion zu?

24. Durch welchen Bestand sollen Mehrfachvergaben ausgeschlossen werden?

25. Wann ist eine Versicherungsnummer wieder zu „löschen“?

26. Wie entsteht die Krankenversicherungsnummer aus der Versicherungsnummer der Rentenversicherung?

6. Versicherungskonto

LERNZIELE

- Sie können den Zweck und den Inhalt von Versicherungskonten erläutern.
- Sie können die rechtlichen Grundlagen für die Führung der Versicherungskonten nennen.

Schon aus der in Abschnitt 2.1 vorgestellten Übersicht über das Rentenversicherungssystem haben Sie zumindest ansatzweise die zentrale Funktion des Versicherungskontos für die Arbeit der Rentenversicherungsträger erkannt. Ohne diese auf maschinell lesbaren Datenträgern gespeicherten Versicherungskonten wäre auch eine vorgestellte Dialogverarbeitung nicht möglich.

6.1 Zweck des Versicherungskontos

In den elektronischen Versicherungskonten, die bei den Rentenversicherungsträgern geführt werden, sind alle rentenrechtlich relevanten Daten gespeichert, die im Laufe des Versicherungslebens anfallen und die zur Feststellung und Erbringung von Leistungen, einschließlich Auskünften aus den Konten, erforderlich sind.

Ziel dieser Speicherung ist es, ein stets aktuelles, vollständiges und richtiges Konto zu haben, um im Leistungsfall den entsprechenden Antrag in der Regel ohne weitere Erhebung bearbeiten zu können. Wesentlich sind diese maschinellen, im Direktzugriff verfügbaren Konten nicht zuletzt auch für den Auskunfts- und Beratungsdienst der Versicherungsträger. Nur durch die Möglichkeit eines dialoggeführten Direktzugriff auf die Versicherungskonten sind die Mitarbeiter im Außendienst auch in der Lage, Cent genaue Rentenauskünfte zu erteilen, bei der Kontenklärung mitzuwirken und den Versicherten individuell zu beraten.

6.2 Rechtliche Grundlagen

Der Bedeutung, die einer normierten und geregelten Führung maschineller Konten für die tägliche Arbeit der Versicherungsträger zukommt, hat auch der Gesetzgeber in verschiedenen Vorschriften Rechnung getragen. Dabei wurden aber nicht nur den Versicherungsträgern Pflichten und Aufgaben zugewiesen, sondern im Interesse einer möglichst hohen Wirtschaftlichkeit und um Reibungsverluste beziehungsweise Medienbrüche zu vermeiden, auch die Versicherten selbst sowie die zuliefernden Stellen, Arbeitgeber, Krankenkassen und so weiter, mit einbezogen.

So verpflichtet zunächst § 149 Absatz 1 SGB VI, für jeden Versicherten ein Versicherungskonto unter einer Versicherungsnummer zu führen. Im Versicherungskonto sind die Daten, die für die Durchführung der Versicherung sowie die Feststellung und Erbringung von Leistungen einschließlich der Rentenauskunft erforderlich sind, zu speichern. Dabei hat der Versicherungsträger darauf hinzuwirken, dass die gespeicherten Daten vollständig und geklärt sind und dass sie auf maschinell verwertbaren Datenträgern mit der Möglichkeit des Direktzugriffes zu speichern sind. Die Versicherten sind durch einen **Versicherungsverlauf** regelmäßig über die in ihrem Konto gespeicherten personenbezogenen Daten, die für die Feststellung der Höhe einer Rentenanwartschaft erheblich sind, zu unterrichten.

Über den geklärten Versicherungsverlauf erhält der Versicherte einen **Feststellungsbescheid.**

Nach § 109 SGB VI erhalten Versicherte, die das 27. Lebensjahr vollendet haben bis zur Vollendung des 55. Lebensjahres jährlich eine schriftliche Renteninformation. In dieser Renteninformation erhält der Versicherte u.a. Auskunft über die Höhe der von ihm, vom

Arbeitgeber und von der öffentlichen Hand für ihn gezahlten Beiträge und über die Höhe der aktuellen Rente. Zusätzlich ist die Höhe der zu erwartenden Regelaltersrente zu prognostizieren. Diese jährlichen Massenverarbeitungen lassen sich nur dann bewältigen, wenn das Versicherungskonto vollständig und fehlerfrei ist.

Allerdings hat der Gesetzgeber dem Versicherten auch Pflichten auferlegt. Im Interesse einer ordnungsgemäßen Kontenklärung sind die Versicherten verpflichtet, bei der Klärung des Versicherungskontos mitzuwirken, den Versicherungsverlauf zu überprüfen, alle für die Kontenklärung erheblichen Tatsachen anzugeben und die notwendigen Unterlagen vorzulegen (§ 149 Absatz 4 SGB VI). Auch die Vorschriften des § 196 SGB VI weisen den Versicherten umfangreiche Auskunfts- und Mitteilungspflichten zu.

Die Versicherungsträger können ihrer aus § 149 Absatz 2 SGB VI resultierenden Pflicht zur Führung vollständiger und geklärter Konten naturgemäß nur dann nachkommen, wenn auch alle relevanten Daten zeitgemäß und richtig von den für die Durchführung der Versicherung zuständigen Stellen geliefert werden. Auch diesem Umstand hat der Gesetzgeber Rechnung getragen und in den §§ 190 ff. SGB VI die Meldung der Versicherungsdaten geregelt. Einzelheiten des Meldeverfahrens sind etwa in der DEÜV sowie der 2. BMeldDÜV festgelegt. Weitere Ausführungen hierzu sind auch im Studientext Nummer 3 „Beitrags- und Meldeverfahren“ enthalten.

6.3 Inhalt des Versicherungskontos

Wir haben in den vorherigen Abschnitten den Zweck des Versicherungskontos sowie die rechtlichen Grundlagen zur Führung der Konten kennen gelernt. Der Inhalt der Versicherungskonten wird von den §§ 149 Absatz 1 und 148 Absatz 1 SGB VI bestimmt. Die erstgenannte Vorschrift fordert nur pauschal, dass „*alle für die Durchführung der Versicherung sowie die Feststellung und Erbringung von Leistungen einschließlich der Rentenauskunft*“ erforderlichen Daten zu speichern sind. Die letztgenannte Vorschrift präzisiert dies dagegen und lässt die Speicherung nur für die „*gesetzlich vorgeschriebenen oder zugelassenen Aufgaben*“ zu.

Die Aufgaben nach dem SGB VI und damit die Daten, die gespeichert werden dürfen, ergeben sich aus der ausschließlichen Aufzählung in § 148 Absatz 1 SGB VI. Hinzu kommen noch Aufgaben aus anderen gesetzlichen Bestimmungen wie Erstattungsverordnungen, den Bestimmungen über den Versorgungsausgleich sowie nicht zuletzt auch den Statistikvorschriften (RSVwV).

Zur Erfüllung der – beispielhaft - aufgezeigten gesetzlichen Aufgaben sind in den Versicherungskonten folgende Datengruppen gespeichert:

- Persönliche Daten einschließlich der Kontoführungsdaten,
- Rentenrechtlich relevante Zeiten,
- Leistungsdaten,
- Daten über den Versorgungsausgleich,
- Daten zur Anerkennung von Zeiten,
- statistische und sonstige Daten.

Zu detaillierteren Beschreibungen der gespeicherten Informationen kann an dieser Stelle auf die anderen Studientexte dieser Reihe verwiesen werden. Bei der Beschreibung der einzelnen Fachverfahren, beispielsweise der Rentenberechnung, wird auf die benötigten Daten und die aus dem Geschäftsprozess neu entstehenden Leistungsdaten näher eingegangen.

ZUSAMMENFASSUNG

- Kapitel 6 beschrieb die Versicherungskonten als Speicherort für alle rentenrechtlich relevanten Daten. Es wurden die rechtlichen Grundlagen zur Führung vollständiger und richtiger Versicherungskonten dargestellt sowie auf die Mitwirkungspflicht der Versicherten bei der Kontenklärung hingewiesen.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

27. Nach welcher Rechtsgrundlage dürfen die Versicherungsträger maschinelle Konten führen?

28. Auf welche Daten ist die Speicherung beschränkt?

29. Welche Datengruppen können in einem Konto vorhanden sein?

30. Welche Datengruppe ist immer vorhanden?

7. Führung der Versicherungskonten, Kontoführungswechsel

LERNZIELE

- Sie kennen die Zuständigkeit für die Kontenführung sowie die Gründe für einen Kontoführungswechsel
- Sie können die Grundzüge des maschinellen Austauschverfahrens bei einem Kontoführungswechsel erklären.

Sie haben aus dem vorhergehenden Kapitel 6 die Bedeutung der Versicherungskonten für die tägliche Arbeit der Versicherungsträger erkannt. Aus Kapitel 5 haben Sie unter anderem auch entnommen, dass durch die Verwendung der Versicherungsnummer als Ordnungsbegriff für die Versicherungskontenführung auch sichergestellt ist, dass für jeden Versicherten grundsätzlich nur ein Konto vorhanden ist.

7.1 Grundsätzliches

Zwischen den Rentenversicherungsträgern sind Regelungen über die Zuständigkeit der Kontenführung und die Art und Weise des Kontenaustausches zwingend erforderlich. Nur so ist einerseits sichergestellt, dass durch eine versichertennahe und zeitnahe Kontenführung auch das erforderliche und angestrebte, ständig auf dem aktuellen Stand befindliche Gesamtkonto erreicht wird. Andererseits stellen die Regeln zum Kontenaustausch und die technischen Einrichtungen sicher, dass die Konten, ohne zeitliche Verzögerung, beispielsweise dem für die Bearbeitung eines Antrages zuständigen Versicherungsträger übermittelt werden.

7.2 Zuständigkeit für die Führung von Versicherungskonten

Die Kontoführung obliegt ausschließlich **einem** Versicherungsträger. Dieser wird auch als **aktueller Kontoführer** bezeichnet. Aktueller Kontoführer ist zunächst stets der Versicherungsträger, der durch die DSRV bei der Vergabe der Versicherungsnummer festgelegt worden ist (§ 127 Absatz1 SGB VI).

Im Bereich der DRV-Bund gibt es Sonderzuständigkeiten, ohne Kontoführer zu sein. Es handelt sich dabei um die Befreiungsanträge der berufsständisch Versorgten und um die Arbeit der Clearingstelle, die die Versicherungspflicht von Selbständigen prüft.

Sofern es sich um einen Handwerker handelt, ist zwingend ein Regionalträger zuständig. Hier erfolgt ein echter Kontoführungswechsel.

Die Zuständigkeit für die Kontoführung richtet sich gemäß § 4 VKVV danach, wer nach den Bestimmungen des SGB VI für die Erfüllung der Aufgaben der Rentenversicherung zuständig ist. Demnach ist ab 01.01.2005 nach § 128 Absatz 1 SGB VI grundsätzlich auch beim Verzug in einen anderen Zuständigkeitsbereich oder ins Ausland ein Kontoführungswechsel angezeigt.

Weitere Anlässe für einen Kontoführungswechsel ab 01.01.2005 können sein:

- Ausgleichsverfahren nach § 274c SGB VI (bis 2019),
- Dauerkontoführung für DRV KBS (Knappschaft, Bahnversicherung oder Seekasse),
- Dauerkontoführung wegen EU-Recht

  sowie

- Eingang eines Geschäftsvorganges bei einem Regionalträger der DRV, wenn der Wohnsitz des Antragstellers im Bereich eines anderen Regionalträgers liegt.

7.3 Kontoführungswechsel

Bei einem Wechsel wird der gesamte Kontoinhalt dem neu zuständigen Versicherungsträger, der dann der aktuelle Kontoführer ist, übergeben (§ 6 Absatz 1 VKVV). Beim abgebenden Versicherungsträger werden nach Abgabe der Daten und nach Eingang einer entsprechenden Empfangsquittung des empfangenden Rentenversicherungsträgers die Daten im bisherigen Versicherungskonto bis auf wenige Identifikationsmerkmale sowie Verweisungsdaten gelöscht (**Rumpfkonto**).

Regeln für den Kontoführungswechsel

Bei der Meldung der Aufnahme einer Beschäftigung (Anmeldung) werden die Daten bei der DSRV u.a. daraufhin geprüft, ob ein Grund für den Wechsel in der Kontoführung vorliegt. Ist die Zuständigkeit der Deutschen Rentenversicherung Knappschaft Bahn See gegeben, wird sie maschinell zur Übernahme des Versicherungskontos aufgefordert (§ 6 Absatz 2 VKVV). Bei einer Änderung der Zuständigkeit zwischen verschiedenen Regionalträgern wird der neu zuständige Versicherungsträger von dem bisher zuständigen Versicherungsträger über die DSRV informiert. Ein Wechsel von einem Regionalträger zum Bundesträger oder umgekehrt ist außerhalb des Ausgleichsverfahrens nach § 274c SGB VI nur in bestimmten Ausnahmen möglich.

Hat ein Versicherter mindestens 1 Monat Versicherungszeit zur DRV KBS geleistet, bleibt diese dauerhaft zuständig. Die Kontoführung wechselt dann im Laufe des Versicherungslebens nicht mehr. Sonderregelungen gibt es auch für die Konten, bei denen das Recht der Europäischen Union anzuwenden ist; hier bleibt die Kontoführung bei der zuständigen Verbindungsstelle. Damit wird den Besonderheiten des Vertragsrechts Rechnung getragen und sichergestellt, dass auch mit den ausländischen Versicherungsträgern eine optimierte Kommunikation erfolgen kann.

Die Zuständigkeit bei der Bearbeitung von Geschäftsvorgängen ist im Dritten Kapitel, Erster Abschnitt des SGB VI (§§126 ff.) beschrieben. Hiernach ist es in nicht seltenen Fällen so, dass die sachliche und örtliche Zuständigkeit im Zeitpunkt der Antragstellung nicht mit der momentan aktuellen Kontoführung übereinstimmt. Zur Bearbeitung von Anträgen benötigt jedoch der zuständige Versicherungsträger zwingend das Gesamtversicherungskonto.

Die Einspeicherung eines Antrages

- in ein aktuelles Konto,
- in ein nicht aktuelles Rumpfkonto

  oder

- die antragsbedingte Kontoeröffnung unter einer bestehenden Versicherungsnummer

  beziehungsweise

- die antragsbedingte Vergabe einer Versicherungsnummer (vergleiche Kapitel 5).

löst daher maschinell eine entsprechende Meldung an die DSRV zur Vormerkung im Stammsatz aus. War in diesem Fall der meldende Versicherungsträger nicht auch aktueller Kontoführer, wird gleichzeitig ein Kontoführungswechsel ausgelöst.

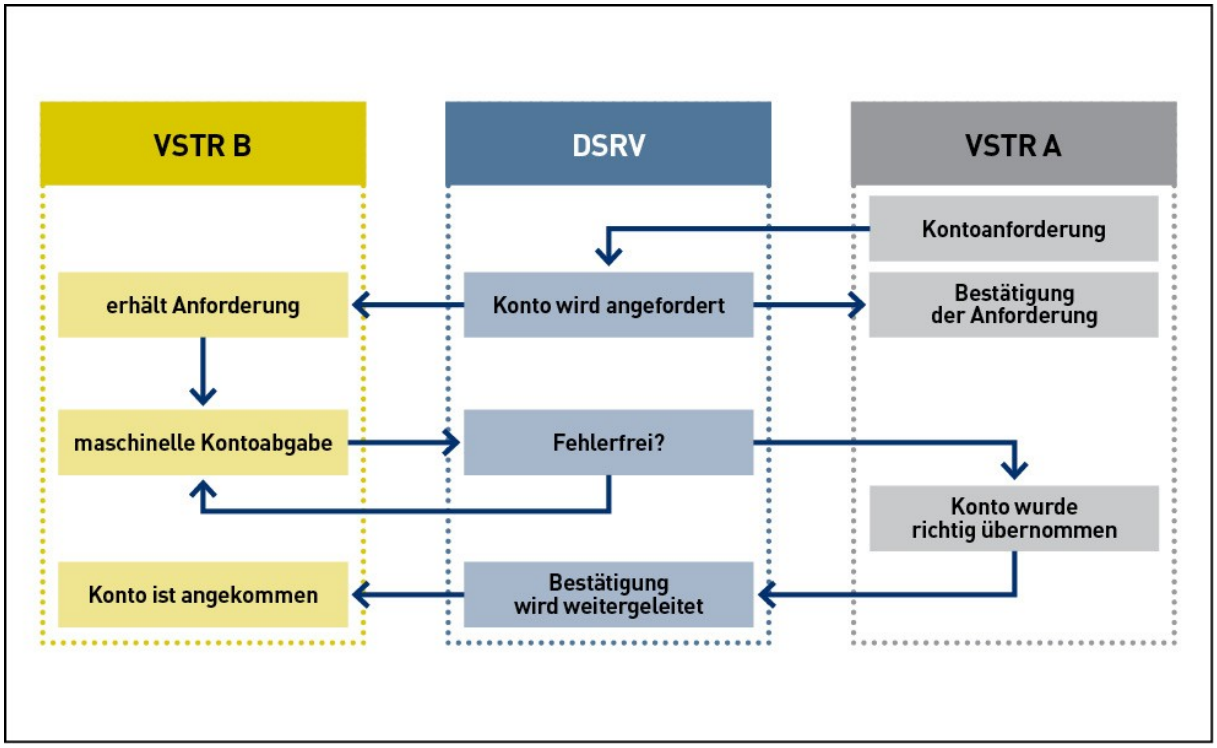
Maschinelles Austauschverfahren

Ebenso wie die Weiterentwicklung der Systeme von der Stapelverarbeitung zur Dialogverarbeitung hat auch die Einführung des maschinellen Austauschverfahrens wesentlich zur Beschleunigung und zur Verminderung des manuellen Arbeitsaufwandes beigetragen.
Während vorher der gesamte Austausch ausschließlich manuell (durch Heraussuchen der Versicherungsunterlagen aus dem Archiv), auf Papier (den Versicherungskarten und Akten) sowie per Post (die Unterlagen mussten auf dem normalen Postweg versandt werden) durchgeführt wurde, erfolgt nunmehr die Kommunikation weitgehend maschinell und elektronisch, ohne Eingriff des Sachbearbeiters und ohne Medienbrüche. Bei all diesen Vorteilen ist größter Wert auf Datensicherheit und Datenschutz gelegt

Sie haben in Kapitel 5 von der zentralen Bedeutung der DSRV im Rahmen der Versicherungsnummernvergabe gehört. Eine ebenso wesentliche Funktion nimmt sie auch im rentenversicherungsinternen Datenaustausch zum Kontoführungswechsel ein. Am Kontoführungswechsel sind insgesamt wenigstens drei Stellen beteiligt und das Verfahren läuft in mehreren koordinierten Einzelschritten in insgesamt drei Phasen ab.

Das Schema in Abbildung 7 zeigt den Kontenaustausch beim Eingang eines Antrags bei einem Versicherungsträger, der zum Zeitpunkt des Antragseingangs nicht aktueller Kontoführer ist. Das Verfahren bei den anderen Anlässen zum Kontoführungswechsel ist weitgehend gleich, allerdings kann der Anstoß auch von der DSRV ausgehen.

Abbildung 7: Schematischer Ablauf des Kontoaustausches



Phase 1 - Kontoanforderung

Der eingehende Antrag wird beim neu zuständigen Versicherungsträger erfasst und im Versicherungskonto dokumentiert oder, falls ein solches noch nicht vorhanden ist, ein neues Versicherungskonto eingerichtet. Auf Grund des eingehenden Antrages wird ein entsprechender Korrespondenzsatz (Anforderungssatz) an die DSRV erstellt. Diese ermittelt aus dem Stammsatz den momentan aktuellen Kontoführer und übermittelt diesem, ebenso als Korrespondenzsatz, eine Aufforderung zur Kontenabgabe. Die Kontoanforderung wird im Stammsatz mit Sender und Empfänger vorgemerkt. Diese Aufforderung zur Kontenabgabe wird beim derzeit noch aktuellen Kontoführer eingespeichert und bewirkt dort eine maschinelle Prüfung des Kontos auf Fehlerfreiheit und eventuelle Verarbeitungs- beziehungsweise Abgabesperren. Der angegangene Versicherungsträger setzt sein Konto auf „Aktuell, Kontoanforderung liegt vor“.

Phase 2 - Kontoübermittlung

Ist das Konto fehlerfrei beziehungsweise sind keine Verarbeitungs- oder Abgabesperren gespeichert, werden die Daten im Konto vom nun abgebenden Versicherungsträger vom internen Speicherformat in das vereinbarte **„DSRV-Austauschformat“** umgeschlüsselt. Der abgebende Versicherungsträger bezeichnet sich im eigenen Konto nunmehr als „Nicht aktuell, Konto abgegeben“. Der abgebende Versicherungsträger baut aus den umgesetzten Daten einen Korrespondenzsatz mit allen Daten des Versicherungskontos auf und übermittelt diesen an die DSRV.

Die DSRV merkt die Kontoabgabe im Stammsatz vor, ermittelt den Empfänger und leitet den Übermittlungssatz an den anfordernden Versicherungsträger weiter. Dieser setzt die Daten aus dem DSRV-Austauschformat wieder in sein internes Speicherformat um, speichert die Daten in das beim Antrag aufgebaute Versicherungskonto und gibt dem Sachbearbeiter eine entsprechende Eingangsquittung. Der - ursprünglich - anfordernde Versicherungsträger bezeichnet sich im Konto nunmehr als „Aktueller Kontoführer“.

Phase 3 - Quittung

Der nunmehr aktuelle Kontoführer quittiert mit einem weiteren Korrespondenzsatz die ordnungsgemäße Übernahme des Kontos.

Die DSRV pflegt entsprechend den Stammsatz (der ursprünglich anfordernde Träger wird nunmehr aktueller Kontoführer, das Verfahren ist abgeschlossen) und leitet die Quittung an den Kontoführer weiter, der das Konto abgegeben hat. Dieser nun nicht mehr aktuelle Kontoführer löscht alle Daten des Kontos bis auf einige Identifikations- beziehungsweise Verknüpfungsmerkmale und führt künftig damit nur noch ein Rumpfkonto.

Das Austauschverfahren ist damit abgeschlossen. Der anfordernde Versicherungsträger hatte innerhalb von ca. drei bis vier Arbeitstagen alle erforderlichen Daten in seinem Versicherungskonto, ohne Eingriff der Sachbearbeitung.

ZUSAMMENFASSUNG

In Kapitel 7 wurden die rechtlichen Grundlagen für die Zuständigkeit zur Kontoführung aufgezeigt sowie das technische Verfahren eines Kontoführungswechsels zwischen den Trägern der Rentenversicherung beschrieben.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

31. Wie wird der für die Kontoführung zuständige Versicherungsträger bezeichnet?

32. Welcher Versicherungsträger ist jeweils als erster für die Kontoführung zuständig?

33. Nennen Sie Gründe für einen Wechsel in der Kontoführung.

34. Nennen Sie die Phasen des Austauschverfahrens.

8. Aktualisierung der Versicherungskonten, Meldeverfahren

LERNZIELE

- Sie können die Grundsätze und die Anlässe für die Aktualisierung der Versicherungskonten nennen.
- Sie kennen die wichtigsten Datenaustauschverfahren zur Aktualisierung der Versicherungskonten und deren Rechtsgrundlagen.
- Sie können das DEÜV-Meldeverfahren aus datentechnischer Sicht erläutern.
- Sie können Aufbau und Sinn der Korrespondenzsätze erläutern und kennen die Gründe für die Dialogisierung des Datenaustausches innerhalb der Rentenversicherung.

Nachdem wir uns in den vorherigen Kapiteln mit dem Ordnungskriterium Versicherungsnummer sowie der Einrichtung der Versicherungskonten und deren Inhalt beschäftigt haben, kommen wir im Weiteren auf die Aktualisierung und Nutzung der Versicherungskonten zu sprechen.

8.1 Zweck des Versicherungskontos und gesetzliche Grundlagen

Sinn und Zweck des Versicherungskontos ist es vor allem, im Leistungs- oder Auskunftsfall die Bearbeitung des Vorganges direkt aus dem Konto heraus erledigen zu können, ohne erneute, zusätzliche Erhebungen durchführen zu müssen. Im Idealfall könnte beispielsweise eine Rentenberechnung vollständig automatisiert ablaufen können.

Dieser Zweck kann nur dann erreicht werden, wenn in den Konten alle relevanten Daten gespeichert und diese auch korrekt sind. Im Rahmen der Datenspeicherung sind aber auch die Bestimmungen des Datenschutzes sowie die jeweiligen Vorschriften zur rechnerischen und sachlichen Feststellung zu beachten.

Unabhängig vom eigenen vitalen Interesse der Versicherungsträger an vollständigen und richtigen Konteninhalten zur Sicherstellung einer effizienten und wirtschaftlichen Aufgabenerledigung ist die Aktualisierung der Versicherungskonten und damit auch die Datenspeicherung von umfangreichen gesetzlichen Vorschriften geregelt.

Basis ist die Verpflichtung der Versicherungsträger zur Führung maschineller Konten, in denen alle rechtserheblichen Daten vollständig und geklärt sind (§ 149 Absatz 1 und 2 SGB VI). Zur Sicherstellung der Richtigkeit und Vollständigkeit ist in regelmäßigen Abständen ein Kontoklärungsverfahren durchzuführen, in dessen Rahmen der Versicherte sowohl einen Versicherungsverlauf als auch einen Feststellungsbescheid erhält (§§ 149 Absatz 3 und 5 SGB VI). Bei der Kontenklärung müssen auch die Versicherten mitwirken (§ 149 Absatz 4 SGB VI).

Die Vorschriften zu den Meldepflichten - §§ 190 ff. SGB VI, §§ 28a ff. SGB IV und die Ausführungsvorschriften in der Datenerfassungs- und -übermittlungsverordnung (DEÜV) - verpflichten die mit der Durchführung der Versicherung befassten Stellen sowie die Meldebehörden, alle Daten unverzüglich und richtig zu melden (Meldeverfahren).

Die Vorschriften der neuen Fassung des Bundesdatenschutzgesetzes (BDSG) sind seit dem 25. Mai 2018 mit der Datenschutz-Grundverordnung (DSGVO) anwendbar und verpflichten die speichernden Stellen, nur richtige und vollständige Daten zu speichern. Zudem ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle) und dass nur befugte Mitarbeiter die gespeicherten Daten verändern oder löschen (Speicherkontrolle) sowie auf die Daten zugreifen können (Zugriffskontrolle).

Letztlich ist nach den - zwar je nach Bundesland verschiedenen, jedoch dem Inhalt nach gleichen - Vorschriften zur Rechnungslegung sicherzustellen, dass nur rechnerisch und sachlich richtige und geprüfte Daten (zum Beispiel über das Vier-Augen-Prinzip) in die Verarbeitung der Rechnungslegung einfließen.

8.2 Anlässe für die Kontoaktualisierung

Unter Berücksichtigung der Vielfalt der im Versicherungskonto enthaltenen Daten - nämlich personenbezogene Daten, das gesamte Versicherungsleben sowie alle Leistungsdaten -, sind naturgemäß auch die Anlässe für die Aktualisierung der Konten sehr vielfältig. Letztendlich müssen alle Sachverhalte, welche die Höhe der Leistung beeinflussen (zum Beispiel alle Beitragszeiten, Anrechnungszeiten, Kindererziehungszeiten) oder die Leistung selbst definieren und darstellen (Rentenart, Leistungsbeginn, Entgeltpunktsummen und so weiter) im Konto enthalten sein.

Unter Berücksichtigung des Grundsatzes, dass die Sachbearbeitung so weit wie möglich maschinell unterstützt wird, insbesondere also die Masse der Daten entweder von außen voll maschinell übernommen beziehungsweise im Rahmen der Verarbeitung maschinell gebildet und gespeichert wird, sind drei Anlässe und Arten der Aktualisierung zu unterscheiden:

- Die **manuelle Bearbeitung** der Versicherungskonten durch die Sachbearbeitung; Diese wird im nächsten Abschnitt erläutert.

- Die **automatisierte Einspeicherung** von Massendaten wie Entgelte und Versicherungszeiten; Die wichtigsten dieser Verfahren zur Kommunikation mit anderen Behörden außerhalb der Rentenversicherung lernen wir in Kapitel 8.4 kennen.

- Die **maschinelle Verarbeitung**; die Ergebnisse aus Verarbeitungsaufträgen der Sachbearbeitung (Rentenbewilligung, Übergangsgeldbewilligung, Nachbehandlungen und so weiter) sowie aus turnusmäßigen Verarbeitungsläufen (monatliche Beitragsabbuchungen, jährliche Rentenanpassungsläufe, regelmäßige Kontoklärungsläufe und so weiter), wie zum Beispiel die Rentenhöhe, Soll-/Ist-Stellungen und Verbuchungen werden im Konto festgehalten. Die aus besonderen Anlässen (zum Beispiel gesetzliche Änderungen, neue Grundsatzurteile, Änderungen in den Datenstrukturen) erforderlichen Bestandsreorganisationen verändern gegebenenfalls den gesamten Kontenbestand.

8.3 Manuelle Pflege

Trotz aller maschinellen Unterstützungen nimmt die Kontoaktualisierung durch die Sachbearbeitung eine nicht unerhebliche Zeit in den Beitrags- und Leistungsabteilungen in Anspruch. Manuell sind die Konten insbesondere aus folgenden Anlässen zu verändern:

- Die **Fehlerbereinigung** der maschinell übermittelten Zeiten aus dem Meldeverfahren (vergleiche Kapitel 8.4) wird vor allem immer dann erforderlich, wenn sich hier Zeiten überschneiden beziehungsweise mit anderen Sachverhalten in unzulässiger Weise zusammentreffen.
  Obwohl auch hier maschinelle Hilfen greifen (maschinelle Termine für eventuelle Berichtigungsmeldungen vormerken, Verschieben von Beginn beziehungsweise Ende von Zeiten bei offensichtlichen Fehlern und so weiter), ist in nicht wenigen Fällen eine manuelle Korrektur nach entsprechender Sachaufklärung erforderlich.

- Die **Einspeicherung** von Sachverhalten, die erst im Rahmen eines Kontoklärungs- beziehungsweise Anerkennungsverfahrens festgestellt werden (Kindererziehungszeiten beziehungsweise Berücksichtigungszeiten, besondere Anrechnungs- und Ersatzzeiten, nach dem FRG beziehungsweise dem SGB VI anerkannte Zeiten und so weiter) sowie die Ergebnisse aus einem durchgeführten Versorgungsausgleich (Bonus beziehungsweise Malus) oder im Rahmen von Beratungsgesprächen erfasste Daten oder Anträge.

- Die **Vorgabe** von Leistungs-, Auskunfts- und Beitragseinzugsdaten, die zur maschinellen (Weiter-) Verarbeitung benötigt werden sowie die Erstellung entsprechender Arbeitsaufträge im Rahmen der Kontenverarbeitung.

- Die nachträgliche Änderung von Leistungsdaten (Abtretungen, Pfändungen, Anschriftenänderungen und so weiter) im Rahmen der **Nachbehandlung**.

Für alle Arten der manuellen Aktualisierung von Konten, also der Eingabe von Daten, stehen in den Rentenversicherungssystemen Eingabemasken, teilweise mit textlichen Erläuterungen sowie Menüführung zur Verfügung. Die manuell vorgegebenen Daten werden grundsätzlich nicht sofort für eine Verarbeitung freigegeben. Sie durchlaufen in jedem Fall zunächst eine Fehlerprüfung. Häufig ist auch bei fehlerfreier Eingabe noch die Freigabe durch einen hierzu berechtigten, anderen Mitarbeiter (Vier-Augen-Prinzip) erforderlich.

Die fehlerfreien und freigegebenen Daten werden im Konto unter der entsprechenden Datengruppe gespeichert. Sie stehen dann bei jeder nachfolgenden Verarbeitung sofort zur Verfügung beziehungsweise lösen weitere maschinelle Verarbeitungen aus.

8.4 Elektronische Kommunikation mit anderen Stellen

Das **Meldeverfahren**, also die Pflicht der mit der Durchführung der Versicherung befassten Stellen (Arbeitgeber, Krankenkasse, Bundesagentur für Arbeit und andere) sowie der Meldebehörden, besondere Meldungen für Zwecke der Rentenversicherung zu übermitteln, ist aus wirtschaftlichen Gründen so angelegt, dass die Daten in der Regel nur einmal erfasst und den anderen Beteiligten im Meldeverfahren anschließend maschinell übermittelt werden. Die wichtigsten elektronischen Meldeverfahren mit anderen Stellen zur Aktualisierung der Versicherungskonten sollen hier kurz vorgestellt werden.

8.4.1 Meldeverfahren nach der DEÜV

Gemeldet und in die Versicherungskonten übernommen werden nach der Datenerfassungs- und -übermittlungsverordnung (DEÜV) insbesondere:

a) Von den Arbeitgebern über die Einzugsstellen der Krankenkassen:

- Beginn und Ende der Beschäftigung,
- Entgelt,
- Sondersachverhalte wie Knappschaft, Bahn, See,
- unständig Beschäftigte
- einmalig gezahltes Entgelt
- Betriebsnummer des Arbeitgebers
- Unterbrechung der Beschäftigung,
- Auflösung der Beschäftigung,
- Jahresmeldungen,
- einmalig gezahltes Entgelt

  sowie
- Berichtigungen,

also Daten, die mit der Beitragspflicht beziehungsweise dem Entgelt in Zusammenhang stehen;

b) von den Krankenkassen, der Bundesagentur für Arbeit (BA) und Rehabilitationsträgern:

- Zeiten der Arbeitsunfähigkeit und Schwangerschaft sowie Schulzeiten,
- Zeiten der Arbeitslosigkeit

  sowie
- Zeiten der Durchführung von Rehabilitationsmaßnahmen,

also alle Zeiten, die entweder Anrechnungszeiten werden, zu beitragsgeminderten Zeiten führen oder bei Beitragszahlung auch zu Beitragszeiten werden.

Im Rahmen dieser DEÜV-Meldungen nimmt die DSRV alle Meldungen von den Meldestellen entgegen. Sie ermittelt aus dem Stammsatz den momentan aktuellen Kontoführer und gibt die Daten an diesen im als Korrespondenzsatz weiter. Der Versicherungsträger speichert diese im Versicherungskonto. Einer Freigabe durch den Sachbearbeiter bedarf es hier nicht. Die Masse der Daten wird damit völlig maschinell in die Konten übernommen.

8.4.2 Sofortmeldungen

Da die Datenstelle der Rentenversicherung als zentrale Meldestelle mit den DEÜV-Meldungen über alle aktuellen Beschäftigungsverhältnisse informiert ist, wurde der Bestand genutzt, um bei Schwarzarbeitskontrollen von Betriebsprüfung und Zoll das Meldeverhalten der Arbeitgeber zu überprüfen. Allerdings muss die Meldung zur Sozialversicherung, eine sogenannte DEÜV-Meldung, erst mit der ersten Entgeltabrechnung des Angestellten erfolgen, spätestens aber innerhalb von sechs Wochen nach Beschäftigungsaufnahme. Eine Aussagekraft über die aktuellen Arbeitsverhältnisse zum Zeitpunkt des

Beschäftigungsbeginns konnte somit nicht gewährleistet werden. Aus diesem Grund wurden zum 1. Januar 2009 für Arbeitgeber, die bestimmten Wirtschaftsbereichen zuzuordnen sind, in denen ein erhöhtes Risiko für Schwarzarbeit und illegale Beschäftigung besteht, die Pflicht zur Abgabe einer Sofortmeldung im Sozialversicherungsrecht eingeführt (§ 28a Absatz 4 SGB IV).
In diesen Bereichen sind für alle Arbeitnehmer Sofortmeldungen zu erfassen. Die Sofortmeldung ist noch vor Beschäftigungsaufnahme vom Arbeitgeber oder dessen Abrechnungsstelle zu erfassen und über eine zertifizierte Schnittstelle direkt an die Datenstelle der Rentenversicherung (ohne Nutzung des DEÜV-Meldeweges über die Krankenversicherung) zu übermitteln. Die Datenstelle der Rentenversicherung nimmt die Sofortmeldungen entgegen, speichert alle relevanten Informationen im Stammsatzbestand und stellt die Sofortmeldungen mittels Webauskunft für die Bekämpfung der Schwarzarbeit und bei der Prüfung der Anmeldung zum Zeitpunkt eines Betriebsunfalls den Berufsgenossenschaften zur Verfügung.
Die Sofortmeldung ersetzt nicht die Meldepflicht nach § 28a Absatz 1 SGB IV (Anmeldung).

8.4.3 Meldeverfahren nach BMeldDÜV

Die 2. Bundesmeldedatenübermittlungsverordnung (2. BMeldDÜV) sieht vor, dass durch die Übermittlung der Einwohnermeldedaten von den Meldebehörden an die Deutsche Rentenversicherung die Aktualität der Angaben in den Versichertenkonten sichergestellt wird.

Diese Datenübermittlung an die Datenstelle der Rentenversicherung (DSRV) erfolgt in automatisierter Form.

Die folgenden Anlässe führen zur Übermittlung von Meldungen durch die Meldebehörden an die DSRV:

- Zuzug aus dem Inland (Zuzug in die Gemeinde)
- Änderung des Namens, des Doktorgrads oder des Geburtsortes
- Änderung der Anschrift (Umzug so weit nicht Zuzug oder Ersterfassung)
- Abmeldung ins Ausland oder nach unbekannt
- Änderung des Geburtsdatums oder des Geschlechts
- Ersterfassung im Melderegister anlässlich des Zuzugs aus dem Ausland
- Meldung nach einer Fehlersituation bei der Meldebehörde
- Rücknahme eines Sterbefalles im Melderegister
- Rücknahme einer Stornierung einer Person im Melderegister
- Ersterfassung im Melderegister auf Grund einer Geburt
- Meldung einer Geburt (an das Konto der Mutter)
- Korrektur einer Meldung einer Geburt (an das Konto der Mutter)
- Löschung der Meldung einer Geburt (an das Konto der Mutter)

• Stornierung einer Person (Löschung aus dem Melderegister)

• Erfassung eines Sterbefalls sowie der Daten zum Ehepartner oder Lebenspartners

• Korrektur eines Sterbefalls

• Rücknahme eines Sterbefalls

• Eheschließungen und/oder Begründung von Lebenspartnerschaften

Die entsprechende Festlegung ist im Kapitel IV.2 der OSCI-XMeld Spezifikation festgehalten.

Gemäß § 6 Absatz 1 der 2. BMeldDÜV übermitteln die Meldebehörden der Datenstelle der Rentenversicherung nach § 150 Absatz 1, § 196 Absatz 2 und 2a des Sechsten Buches Sozialgesetzbuch sowie § 36 DEÜV zur Ermittlung möglicher Leistungsansprüche, zur Vermeidung unrechtmäßiger Erbringung von Geldleistungen und zur Aktualisierung von Versicherten- und Mitgliederbeständen oder zum Zwecke der Aktualisierung der bei den Trägern der Deutschen Rentenversicherung gespeicherten Daten unverzüglich folgende Daten in automatisierter Form:

1. Familienname

2. frühere Namen

3. Vornamen

4. Doktorgrad

5. Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat

6. Geschlecht

7. derzeitige Anschrift

7a. bei Wegzug in das Ausland, soweit möglich, die Zuzugsanschrift im Ausland und der Staat

8. bei Änderung der Anschrift die letzte frühere Anschrift

9. Datum der letzten Eheschließung oder der letzten Begründung einer Lebenspartnerschaft

10. Sterbedatum

Im Sterbefall übermitteln die Meldebehörden der Datenstelle der Rentenversicherung zusätzlich zu den Daten nach Absatz 1 folgende Informationen:

1. Ehegatte – Familienname

2. Ehegatte – Vornamen

3. Ehegatte – Geburtsdatum

4. Ehegatte – derzeitige Anschrift der alleinigen Wohnung oder der Hauptwohnung

5. Lebenspartner – Familienname

6. Lebenspartner – Vornamen

7. Lebenspartner – Geburtsdatum

8. Lebenspartner – derzeitige Anschrift der alleinigen Wohnung oder der Hauptwohnung

Diese Daten werden von der DSRV taggleich an den zuständigen Rentenversicherungsträger, die Krankenkasse als zuständige Einzugsstelle (sofern diese der DSRV bekannt ist), die Bundesagentur für Arbeit und die Minijobzentrale weitergegeben.

Darüber hinaus sind auch die Mitteilungen über Sterbefälle nach § 101a SGB X von den Meldebehörden an die DSRV zu übermitteln. Diese leitet die Sterbedaten unverzüglich an den Renten Service der Deutschen Post AG weiter. Dieser stellt dann ggf. die Rentenzahlung ein und der zuständige Rentenversicherungsträger wird über eine Mitteilung an den Leistungsträger vom Renten Service informiert.

Datenübermittlung im XMeld Verfahren über OSCI

Das XMeld Verfahren (Verfahren Datenaustausch mit den Meldebehörden) nutzt den Standard OSCI.

Online Services Computer Interface (OSCI) sind Protokollstandards für den sicheren elektronischen Nachrichtenaustausch über das Internet und andere Netze. Sie garantieren Integrität, Authentizität, Vertraulichkeit und Nachweisbarkeit der Daten und ermöglichen ihre medienbruchfreie, effiziente Verarbeitung.

OSCI ermöglicht den elektronischen Austausch von Nachrichten und Dokumenten mit besonders hohen Sicherheitsanforderungen innerhalb und mit der öffentlichen Verwaltung. Der Einsatz von OSCI ist für die Kommunikation mit den Behörden verbindlich.

Über OSCI können Behörden miteinander, mit Unternehmen und mit Bürgerinnen und Bürgern automatisiert Dateien und Informationen austauschen. Im Verfahren XMeld erfolgt der Datenaustausch über XML-Dateien zwischen den Meldebehörden und der Datenstelle der Träger der Rentenversicherung (DSRV).

OSCI wird im Auftrag des IT-Planungsrates von der Koordinierungsstelle für IT-Standards (KoSIT) betrieben.

Halbjährlich gibt es im Verfahren einen Releasewechsel auf eine neue OSCI-XMeld-Spezifikation, welche von der DSRV und den Verfahrensherstellern umgesetzt wird. Dieser Releasewechsel findet jeweils zum 01.05 und 01.11. statt.

8.4.4 Maschinelles Meldeverfahren zur Krankenversicherung der Rentner (KVdR) und zur Pflegeversicherung

Aus den §§ 201 Absatz 1 SGB V, 247 SGB V und 39 Absatz 3 KVLG ergeben sich für die Krankenkassen und die Rentenversicherungsträger eine Reihe von Meldepflichten hinsichtlich der gesetzlichen Krankenversicherung und der sozialen Pflegeversicherung. Insbesondere im Rahmen der Rentenantragstellung, der Entscheidung über den Rentenantrag sowie im Laufe des Rentenbezugs ergibt sich ein sehr intensiver Kommunikationsbedarf zwischen den Sozialleistungsträgern.

Der Datenaustausch erfolgt nicht direkt zwischen dem Rentenversicherungsträger und der zuständigen Krankenkasse, sondern über die zuständige Weiterleitungsstelle der Krankenkasse (= zentrale Datensammel-, -verteil- und -weiterleitungsstellen) und der Datenstelle der Rentenversicherung. Der Aufbau und Inhalt der Datensätze sind in einer gemeinsamen Datensatzbeschreibung festgelegt.

Auf Antrag wird von der zuständigen Krankenkasse das Krankenversicherungsverhältnis geprüft. Sodann wird ein Datensatz mit allen relevanten Daten zum Versicherungsverhältnis an den Rentenversicherungsträger abgesetzt. Dieser speichert die von der Krankenkasse gemeldeten Daten im Versicherungskonto, gestaltet die Abführung der Krankenversicherungs-beiträge aus der Rente entsprechend des gemeldeten Versicherungsverhältnisses und übermittelt einen entsprechenden Datensatz an die zuständige Krankenkasse. Vom Rentenversicherungsträger sind Tatbestände zu melden, die das Krankenversicherungsverhältnis beeinflussen können, wie z.B. die Bewilligung einer Rente oder eine Beschäftigungsaufnahme.

8.4.5 Maschinelles Erstattungsverfahren (EA – Verfahren)

In den Paragrafen §§102 – 105 SGB X werden Erstattungsansprüche der Leistungsträger untereinander geregelt. Mit dem 7. SGB – Änderungsgesetz wurde die gesetzliche Verpflichtung normiert, dass Erstattungsansprüche der gesetzlichen Krankenversicherung oder der Bundesagentur für Arbeit gegenüber den Trägern der gesetzlichen Rentenversicherung ab dem 01.08.2023 verpflichtend elektronisch zu übermitteln sind.

Folgende Meldungen wurden somit von papierhaft auf elektronisch umgestellt:

- Anmeldung eines Erstattungsanspruches
- Mitteilung über die Leistungsgewährung oder Leistungsablehnung
- Bezifferung eines Erstattungsanspruches
- Abrechnung eines Erstattungsanspruches

Ein Beispiel für einen Erstattungsanspruch stellt die Überschneidung von Krankengeld und Rentenzahlung dar.

Fällt der Anspruch auf Krankengeld mit dem Bezug einer Rente zusammen, so ist der Anspruch auf Krankengeld teilweise oder ganz entfallen. Somit erwirbt die Krankenkasse einen Erstattungsanspruch gegenüber dem Rentenversicherungsträger und ist erstattungsberechtigt. Der Rentenversicherungsträger ist in diesem Fall erstattungspflichtig.

Wird eine mögliche Erstattungspflicht nach dem SGB X festgestellt, erfolgt eine unverzügliche Anmeldung des Erstattungsanspruchs durch den erstattungsberechtigten Träger beim erstattungspflichtigen Träger. Nach Prüfung der übermittelten Daten unterrichtet der erstattungspflichte Träger den erstattungsberechtigten Träger über die Leistungsgewährung beziehungsweise die Leistungsablehnung in Form einer Mitteilung.

Liegt ein Erstattungsanspruch vor, wird er gegenüber dem erstattungspflichtigen Sozialversicherungsträger beziffert, ansonsten erfolgt eine Fehlanzeige oder Unzuständigkeitserklärung. Nach Eingang der Bezifferung nimmt der erstattungspflichtige Träger die Abrechnung vor und leitet diese an den erstattungsberechtigten Träger weiter.

Perspektivisch soll zukünftig jegliche Kommunikation in Bezug auf Erstattungsansprüche nach §§ 102 ff. SGB X zwischen den Leistungsträgern elektronisch erfolgen.

Der Datenaustausch erfolgt nicht direkt zwischen dem Rentenversicherungsträger und dem zuständigen Leistungsträger, sondern über die zuständigen Weiterleitungsstellen der Krankenkassen (= zentrale Datensammel-, -verteil- und -weiterleitungsstellen), der Bundesagentur für Arbeit und der Datenstelle der Rentenversicherung.

Der Aufbau und Inhalt der Datensätze sowie die Meldetatbestände sind in einer gemeinsamen Verfahrensbeschreibung vereinbart worden.

8.4.6 Rentenzahlungen durch den Renten Service der Deutschen Post AG

Nach § 119 Absatz 1 Satz 1 SGB VI werden die laufenden Geldleistungen der Träger der allgemeinen Rentenversicherung – mit Ausnahme des Übergangsgeldes – durch die Deutsche Post AG ausgezahlt.

Im Übrigen können die Träger der Rentenversicherung Geldleistungen durch die Deutsche Post AG auszahlen lassen (§ 119 Absatz 1 Satz 2 SGB VI). Von dieser Möglichkeit macht die Deutsche Rentenversicherung Knappschaft-Bahn-See für Zahlungen aus der knappschaftlichen Rentenversicherung ins Ausland seit dem Arbeitsmonat Mai 2011 Gebrauch. Seit dem Rentenauszahlungstag am 28. April 2023 werden ebenfalls alle inländischen Renten der Deutschen Rentenversicherung Knappschaft-Bahn-See über die Deutsche Post AG ausgezahlt, so dass seit diesem Zeitpunkt **alle** Renten der gesetzlichen Rentenversicherung durch den Renten Service der Deutschen Post AG ausgezahlt werden. Ebenso wie viele andere Verfahren wird auch das Postzahlverfahren sowohl seitens der Rentenversicherungsträger als auch der Deutschen Post AG im Rahmen eines maschinellen Datenaustausches abgewickelt. So wie der Auftrag für die Rentenzahlung sowie alle späteren Änderungen, mit Ausnahme der normalen Rentenanpassungsänderungen, vom Leistungsträger der Post auf maschinellem Wege übermittelt werden, gibt auch der Renten Service alle ihm bekannt gewordenen und von ihm durchgeführten Änderungen auf maschinellem Weg an die Leistungsträger zurück. Insbesondere sind dies außerhalb der Rentenanpassungsarbeiten:

- Änderungen in den Anschriften,
- Änderungen der Bankverbindungen

  sowie

- Zahlungseinstellungen wegen Tod des Berechtigten.

Auch diese Daten werden maschinell in die Konten übernommen.

8.4.7 Datenaustausch mit den Kliniken

Speziell für den Datenaustausch mit den Kliniken im Zusammenhang mit der Durchführung von Rehabilitationsmaßnahmen wurde ein eigenes Datenaustauschverfahren entwickelt. Im Rahmen dieses Verfahrens melden die Rentenversicherungsträger den durchführenden Rehabilitationskliniken die Daten der bewilligten Maßnahme (persönliche Daten des Patienten, Kostenträgerdaten, Diagnosen, medizinische Hinweise und so weiter). Ebenso liefern die Kliniken alle Durchführungsdaten (Aufnahme, Entlassung, Kosten, Verlängerung, Unterbrechungen und so weiter) maschinell zurück.

Diese Daten werden ebenfalls maschinell in die Konten übernommen und automatische Folgeverarbeitungen ausgeführt. So erfolgen beispielsweise die Zahlung des Übergangsgeldes, die Abrechnung von Pflegekosten sowie die statistischen Meldungen voll maschinell.

Zudem sind die Rentenversicherungsträger, die ein nach § 108 SGB V zugelassenes Krankenhaus betreiben, nach § 301 SGB V verpflichtet verschiedene Daten zur Krankenhausbehandlung auf maschinellem Wege den Krankenkassen zu übermitteln.

Mit einem damit hergestellten Kommunikationsweg von Krankenkassen zu Kliniken, sowie Rentenversicherungsträger zu den Kliniken, konnte damit das Mitteilungsverfahren nach §301 Absatz 4a SGB V ebenfalls in diesem Datenaustausch integriert und die Kommunikation zwischen RV-Träger und Krankenkassen eingerichtet werden.

Eine Rahmenvereinbarung mit ihren technischen Anlagen, die vom GKV-Spitzenverband in Absprache mit der DRV und den Kliniken gepflegt werden, sorgen für eine immer aktuelle Dokumentation.

8.4.8 Rentenbezugsmitteilungsverfahren und Maschinelles Anfrage Verfahren zur Übermittlung der steuerlichen Identifikationsnummer

Die gesetzliche Rentenversicherung ist – ebenso wie alle anderen Institutionen in Deutschland, die Rentenzahlungen leisten (zum Beispiel Banken und Versicherungen) – gesetzlich verpflichtet, im Rentenbezugsmitteilungsverfahren der Finanzverwaltung eine elektronische Mitteilung über geleistete Rentenzahlungen zu übermitteln (Rebsy).

Damit die übermittelten Daten den zuständigen Stellen in der Finanzverwaltung zugeordnet werden können, muss die Deutsche Rentenversicherung die sogenannte steuerliche Identifikationsnummer in die Rentenbezugsmitteilung eintragen. Diese Nummer wurde ab August 2008 jedem Bürger in Deutschland vom Bundeszentralamt für Steuern mitgeteilt.

Um das Verfahren für die Rentnerinnen und Rentner möglichst unbürokratisch zu gestalten, fragt die gesetzliche Rentenversicherung (aufgrund einer gesetzlichen Ermächtigung und

entsprechend den datenschutzrechtlichen Vorgaben) bei dem Bundeszentralamt für Steuern die steuerliche Identifikationsnummer an und speichert diese dann im Rentenversicherungskonto über ein maschinelles Anfrage Verfahren (MAV) ab.

8.4.9 Zulageverfahren Pflegeversicherung

Mit Einführung des Gesetzes zur Neuausrichtung der Pflegeversicherung wurde die Möglichkeit geschaffen, dass Versicherte der gesetzlichen Pflegeversicherung künftig eine Zulage in Höhe von 60 € jährlich zu ihrer Versicherungsprämie erhalten, wenn sie eine freiwillige, private Pflege-Zusatzversicherung abschließen. Diese Pflegevorsorgezulage wird auf Antrag durch eine zentrale Stelle bei der DRV Bund gewährt.

In diesem Antrag ist die Versicherungsnummer der zulageberechtigten Person anzugeben. Sofern eine Versicherungsnummer noch nicht vergeben wurde, vergibt die zentrale Stelle zur Erfüllung ihrer zugewiesenen Aufgaben eine Zulagennummer. Nach den gesetzlichen Regelungen ist es zulässig, dass die zentrale Stelle die Datenstelle der Rentenversicherung (DSRV) beauftragt, für das Zulageverfahren Pflegeversicherung (ZVP) und der damit verbundenen Aufgaben nach dem Sozialgesetzbuch eine Versicherungsnummer zu vergeben. Diese Versicherungsnummer ist von der zentralen Stelle als Zulagennummer zu verwenden.

Die Realisierung des Verfahrens zur Vergabe einer Versicherungsnummer als Zulagennummer wird weitestgehend analog zum Verfahren zur Vergabe einer Versicherungsnummer durch externe Stellen beziehungsweise zur Vergabe einer Versicherungsnummer auf Basis der Krankenversichertennummer - also auf Basis bestehender Verfahren - realisiert. Die Vergabe einer Versicherungsnummer als Zulagennummer im Zulageverfahren Pflegeversicherung entspricht der Vergabe einer Versicherungsnummer auf Basis der Krankenversichertennummer.

Aufgrund der gesetzlichen Erfordernisse startete das Verfahren zwingend zum 01.01.2014. Im Zusammenhang mit der Einführung dieses Verfahrens musste unter anderem das Verfahren für die Vergabe einer Versicherungsnummer bei der DSRV angepasst und erweitert werden. Die Mitteilung über die Vergabe einer Versicherungsnummer als Zulagennummer erfolgt von der DSRV an die zentrale Stelle und von dort an die Versicherten. Die Ausstellung eines Versicherungsnummernachweises erfolgt nicht.

8.4.10 Digitale Verfahren zur Beitragssatzdifferenzierung in der sozialen Pflegeversicherung (DaBPV)

Durch das Pflegeunterstützungs- und -entlastungsgesetz (PUEG) ist für Zeiten seit dem 1. Juli 2023 eine Differenzierung des Beitragssatzes in der sozialen Pflegeversicherung nach der Kinderanzahl eingeführt worden. Dies geht auf ein entsprechendes Urteil des Bundesverfassungsgerichts zurück.

Um eine einheitliche Rechtsanwendung sicherzustellen und ein möglichst effizientes, schnelles und bürgerfreundliches Verwaltungshandeln zu gewährleisten, wurde ab dem 1. April 2025 ein digitales Verfahren zur Erhebung und zum Nachweis der Anzahl der berücksichtigungsfähigen Kinder bereitgestellt. Zu diesem Zweck steht den beitragsabführenden Stellen das automatisierte Datenaustauschverfahren zur Beitragssatzdifferenzierung in der sozialen Pflegeversicherung (DaBPV) zur Verfügung. Die Teilnahme am DaBPV-Verfahren ist für alle beitragsabführenden Stellen, die zur Berücksichtigung von Zu- und Abschlägen verpflichtet sind und für Zahlstellen und Pflegekassen obligatorisch.

In enger Abstimmung mit dem Bundeszentralamt für Steuern (BZSt), der DRV Bund und dem GKV-Spitzenverband wurde zum gesetzlichen Einsatztermin am 1. April 2025 das digitale Verfahren erfolgreich an den Start gebracht. Es wurde ein automatisiertes Datenaustausch- und Weiterleitungsverfahren realisiert, bei dem die DSRV gemäß den Vorgaben der § 55a SGB XI und 28a SGB IV über die Zentrale Zulagenstelle für Altersvermögen (ZfA) für die beitragsabführenden Stellen (RV-Träger, Arbeitgeber und Zahlstellen) beim Bundeszentralamt für Steuern die Kinderzahl der Beschäftigten abfragt.

Das neue digitale Verfahren zur Erhebung und zum Nachweis der Anzahl der berücksichtigungsfähigen Kinder zur Beitragsdifferenzierung nach Kinderzahl in der sozialen Pflegeversicherung nach § 55 Absatz 3c Satz 1 SGB XI berücksichtigt die Prinzipien „Once Only“ und „Digital Only“. Circa 80 Millionen initiale Abfragen, davon 21 Millionen Bestandsanfragen allein von den RV- Trägern, laufen elektronisch über bestehende Kommunikationswege. Ab April 2025 bis Ende des Jahres 2025 wurden ca. 160 Millionen

Datensätzen ausgetauscht. Diese hohe Zahl ergibt sich daraus, dass ca. 80 Millionen initiale Anfragen über die DSRV und die ZfA an das BZSt sowie ca. 80 Millionen initiale Rückmeldungen auf die Anfragen übermittelt wurden. Danach wird von einem jährlichen Anfragevolumen von ca. 25 Millionen Datensätzen und genauso vielen Antworten ausgegangen zzgl. 3 Millionen Push-Meldungen, die durch das BZSt im sog. Push-Verfahren ausgelöst werden. Bei diesem wird ein Abonnement eingerichtet – bei sich ändernder Kinderzahl und entsprechender Anmeldung erfolgen durch das BZSt proaktive Änderungsmeldungen an die beitragsabführende Stelle für die von ihnen angemeldeten beitragspflichtigen Arbeitnehmer.

8.5 Fehlerprüfung und Freigabeverfahren

Alle eingehenden Daten, ob sie manuell hinzukommen oder aus maschinellen Meldungen stammen, werden umfangreichen maschinellen Fehlerprüfungen unterworfen. Diese unterteilen sich in:

- Plausibilitätsprüfungen, die die Fehlerfreiheit der einlaufenden Daten in sich sicherstellen (Richtigkeit der Schlüssel, zulässige Daten, Prüfung der Feldinhalte gegen zentrale Dateien wie PLZ-Datei, BLZ-Datei, Diagnosedateien und so weiter),

- Querverbindungsprüfungen, die sicherstellen, dass die eingehenden Daten auch zu den bereits gespeicherten beziehungsweise anderen einlaufenden Daten schlüssig sind. Darunter fallen Prüfungen auf fehlende Zeiten vor dem Eintritt in die Versicherung, keine Zeiten in die Zukunft, keine Zeitüberschneidungen, keine FRG-Zeiten ohne Herkunftsland.

- Wartezeit- und Voraussetzungsprüfungen, auf deren Basis kontrolliert wird, ob Rahmenbedingungen eingehalten werden, so dass beispielsweise für die vorgegebene Rentenart auch die Wartezeit erfüllt ist oder sonstige versicherungsrechtliche Voraussetzungen erfüllt sind.

Ein eventuell erkannter Fehler führt zu einer Verarbeitungssperre für das betroffene Konto. Eine Verarbeitung ist daher erst dann möglich, wenn der Fehler bereinigt ist. Hierzu erfolgt sofort beim Einlaufen der Daten eine entsprechende Fehleranzeige, im Dialogbetrieb am Bildschirm, ansonsten durch einen schriftlichen Fehlerhinweis.

8.6 Datenschutz

Auch die Einhaltung des Datenschutzes sowie des Vier-Augen-Prinzips wird durch umfang reiche Programmkomplexe sichergestellt.

Die Berechtigungsprüfung beginnt damit, dass sich der Bearbeiter vor der Arbeit am Rechner gegenüber dem System identifizieren muss. Maschinelle Routinen stellen sicher, dass dieser Mitarbeiter nur die Konten bearbeiten kann, die in seinen Zuständigkeitsbereich fallen (**Zugriffskontrolle**) und auch nur die Daten lesen, verändern, eingeben oder löschen kann, die seinem Aufgabenbereich zugeordnet sind (**Speicherkontrolle**). Eventuell unzulässige Zugriffe oder Eingaben werden abgewiesen.

Die berechtigt vorgenommenen Eingaben werden maschinell mit den Personalien des Eingebers verbunden. Hierzu wird aus den Identifikationsmerkmalen bei der Anmeldung ein **Verursachersatz** maschinell zu allen Kontoveränderungen gebildet. Dieser steht für spätere (Stichproben-) Kontrollen zum Beispiel durch die internen Datenschutzbeauftragten zur Verfügung.

Das Vier-Augen-Prinzip wird dadurch realisiert, dass alle diesem Prinzip unterworfenen eingegebenen Daten zunächst als „nicht freigegeben“ gekennzeichnet sind. Das heißt, eventuelle Verarbeitungen würden ohne diese Daten stattfinden beziehungsweise Verarbeitungsaufträge würden nicht wirken. Erst wenn diese Eingaben von einer anderen, hierzu berechtigten Person, die sich natürlich ebenso identifizieren muss, geprüft und freigegeben wurden, sind sie maschinell relevant. Die Kennzeichnung der freizugebenden Daten als „geprüft und freigegeben“ erfolgt durch Eingabe eines Kommandos beziehungsweise Arbeitsauftrages. Es wird die Prüfnummer des Erfassers und des Freigebers gespeichert.

Technische Verfahren

Die zum Datenaustausch eingesetzten technischen Verfahren sind vielfältig. Für den Massenaustausch zum Beispiel im Rahmen des DEÜV-Verfahrens zwischen den Sozialleistungsträgern findet häufig aus Performancegründen ein File Transfer statt. Das SSH File Transfer Protocol oder Secure File Transfer Protocol (sFTP) ist ein Netzwerkprotokoll zur verschlüsselten Übertragung von Dateien über TCP/IP-Netzwerke. Es wird benutzt, um Dateien zwischen zwei Endgeräten/Rechnern zu übertragen.

Zum Einsammeln der Daten vom Meldepflichtigen wird eine breite Palette von Möglichkeiten zur Verfügung gestellt. Auf einige Möglichkeiten, die das Internet bietet, kommen wir in Kapitel 10 zurück. So gibt es für die DEÜV-Meldungen das SV-Meldeportal (im Internet https://www.itsg.de/produkte/sv-meldeportal/).

Zur Kommunikation mit den Arbeitgebern, beziehungsweise deren Softwareherstellern der Lohn- und Gehaltsprogramme kommen vereinbarte Meldewege wie DAKOTA (verschlüsselte E-Mail) oder der eXTra-Standard zum Einsatz.

Der erweiterte XML-Transportstandard (eXTra-Standard) ist eine frei verfügbare Beschreibung eines Transportverfahrens, das für den Datenaustausch zwischen Wirtschaft und Verwaltung konzipiert wurde. An der Erstellung des Standards waren unter anderem die Arbeitgeber, die DATEV, die DSRV, die Gesetzliche Krankenversicherung und das Statistische Bundesamt beteiligt. eXTra richtet sich insbesondere an bereits bestehende oder geplante Datenübermittlungsverfahren zwischen Wirtschaft und Verwaltung sowie innerhalb der Wirtschaft. eXTra als technisches Transportverfahren fordert keinerlei Bedingungen für die Teilnahme; ausschließlich die Datenübermittlungsverbünde beziehungsweise die unterstützten Fachverfahren regeln die Teilnahmeberechtigungen.

Mit anderen Behörden finden elektronische Postfächer, in denen Meldungen gesammelt und dann gemeinsam abgerufen werden können, oder im Rahmen der E-Government-Initiative der Bundesregierung 2005 geschaffene Standards wie die Virtuelle Poststelle (VPS) Anwendung. Auf breiter Basis werden zudem Datensatznormierungen im XML-Format verwendet.

Aber auch innerhalb der Rentenversicherung müssen die Informationen fließen. Grundlage hierzu ist einerseits das Datennetz der Deutschen Rentenversicherung (siehe Kapitel 3) über welches der eigentliche Datentransport abgewickelt wird. Andererseits bedarf es auch hier gemeinsamer Verfahrensgrundsätze, die als DSRV-Verfahren bezeichnet werden.

8.7 Datenaustausch innerhalb der Deutschen Rentenversicherung

Wir wissen aus den vorherigen Kapiteln bereits, dass bisher zwei unterschiedliche Programmsysteme in der Rentenversicherung existierten, die sich bei weitgehend gleichem Funktionsumfang insbesondere durch die interne Speicherform und Darstellung der Versicherungskonten unterschieden haben. Die beiden Programmsysteme wurden durch ein gemeinsames Programmsystem - rvDialog - abgelöst. Darüber hinaus haben Sie im vorstehenden Abschnitt erfahren, dass eine der wesentlichsten Funktionen des Datenaustausches und einer seiner größten Vorteile darin liegt, dass die Daten völlig maschinell, ohne Medienbrüche beziehungsweise Eingriff der Sachbearbeitung von Konto zu Konto übermittelt werden.

Austauschschlüssel und DSRV-Verfahren

Für den Datenaustausch zwischen den Rentenversicherungsträgern hat man sich auf das gemeinsame „**DSRV-Austauschformat“** und entsprechende Datensätze verständigt (**DSRV-Verfahren**). In Summe handelt es sich hierbei um ein neutrales Schlüsselsystem. Im Falle eines Datenaustausches zwischen zwei Versicherungsträgern setzt der absendende Versicherungsträger die Daten aus seinem internen Speicherformat in das DSRV-Austauschformat um. Der empfangende Versicherungsträger ist ohne weiteres maschinell in der Lage, aus diesem normierten Format in sein eigenes Format zu konvertieren. Nachdem grundsätzlich das gesamte Versicherungskonto ausgetauscht werden kann, entspricht das Schlüsselspektrum für die zu speichernde Sachverhalte weitgehend dem der jeweiligen internen Speicherformen.

Korrespondenzsätze

Auf das Schlüsselverzeichnis selbst braucht im Rahmen dieses Studientextes nicht eingegangen zu werden. Es soll jedoch das Format der Korrespondenzsätze kurz erläutert werden, da dieser Grundaufbau stets gleich ist, unabhängig davon, welche Informationen ausgetauscht werden.

Der Korrespondenzsatz besteht aus einem festen und einem variablen Teil. Im festen Teil sind neben dem Ordnungsbegriff Versicherungsnummer und ggf. weiterer persönliche Daten zum Versicherten insbesondere der Absender sowie Angaben zum Inhalt des variablen Teils enthalten. Unterschiedliche Verfahren und Sachverhalte werden über ein Satzkennzeichen (SK) beschrieben (zum Beispiel Kontoanforderung SK=50; Aufbau- oder Merkmalssatz SK=51, und so weiter). Die einzelnen Sachinformationen, zum Beispiel die Zeiten, Anträge, persönliche Informationen und so weiter, sind dann in der jeweils erforderlichen Anzahl in einer variablen Ablage angefügt. Der Informationsgehalt der variablen Ablage, das heißt, welche Information sich dahinter verbirgt (wie Entgelt für ein volles Jahr, Krankheit mit Von/Bis-Datum, Herkunftsland und so weiter) wird jeweils durch einen dreistelligen Formatschlüssel definiert.

Die Einführung der DEÜV ab 1.1.1999 enthielt verschiedene Neuregelungen für das Meldeverfahren. Die Inhalte der Datenübermittlung zwischen Arbeitgebern und Krankenkassen folgen einem ähnlichen Aufbau wie die Korrespondenzsätze mit fixen Datensätzen (DSxy) und einzelnen Datenbausteinen (DBxy) zu bestimmten Sachverhalten und werden heute auch im Rahmen des DSRV-Verfahrens eingesetzt.

Bei der Kommunikation mit externen Stellen hat der Austausch über normierte XML-Datenstrukturen (XML=Extensible Markup Language; englisch für „erweiterbare Auszeichnungssprache“) an Bedeutung gewonnen. Ein XML-Schema entspricht einer Datensatzbeschreibung und ist eine hierarchische Datenstruktur in XML, die in Form von Textdaten beschrieben wird und eine große Anzahl von Datentypen unterstützt.

Dialogisierung

Von großer Bedeutung für die Versicherten der Rentenversicherung ist die Möglichkeit, sich zu jeder Zeit über den Stand ihrer Versorgung im Alter informieren zu können. Dies soll möglichst unkompliziert und ohne allzu großen Aufwand für die Versicherten und auch für den Rentenversicherungsträger von statten gehen. Den Versicherten selbst interessieren die hierzu gesetzlich festgelegten Zuständigkeitsregelungen wenig. Er möchte seine Auskünfte am liebsten von der nächstgelegenen Auskunfts- und Beratungsstelle der Rentenversicherung oder über einen Online-Dienst der Rentenversicherung erhalten. Damit ist auch schon der Kern der Dialogisierung erklärt, nämlich die sofortige **Auskunft für jeden Versicherten an jeder beliebigen Auskunfts- und Beratungsstelle oder über das Internetangebot der Deutschen Rentenversicherung**.

Durch den im RVOrgG festgelegten Übergang der Auskunfts- und Beratungsstellen auf die Regionalträger, wurde die Notwendigkeit besonders deutlich, aktuelle Informationen online und sofort von einem Versicherungsträger zum anderen übersenden zu können. Dabei muss ggf. eine Konvertierung beziehungsweise Aufbereitung der Daten erfolgen.

Zur Realisierung der hierfür erforderlichen „**Dialogisierung** des Datenaustausches zwischen den Trägern der gesetzlichen Rentenversicherung“ können unter Nutzung des bereits vorhandenen Leitungsnetzes auf elektronischem Wege über die Datenstelle der Rentenversicherung u.a. folgende Auskünfte im Dialog angefordert werden:

- Versicherungsverläufe (mit und ohne Lückenhinweise),
- Lückenauskunft,
- Rentenauskünfte „Erwerbsminderung“,
- Rentenauskünfte „Altersrente“,
- Renteninformation,
- Rentenbezugsmitteilungen zur Vorlage beim Finanzamt.

Daneben sind weiter Verfahren integriert worden, um gegenüber dem Datenaustausch im normalen DSRV-Verfahren die Geschwindigkeitsvorteile einer Dialogverarbeitung nutzen zu können (zum Beispiel Online-Vergabe, Online-Update, Kontoführungswechsel im Dialog).

Da aus datenschutzrechtlichen Gründen sowohl den Auftraggeber (anfordernder Rentenversicherungsträger) wie auch den Auftragnehmer (abgebender Rentenversicherungsträger) die Verpflichtung trifft, Sozialdaten der Versicherten nur Befugten zugänglich zu machen, wurde festgelegt, dass eine Protokollierung des Zugriffs beim jeweiligen Versicherungsträger zu erfolgen hat.

Der Austausch der Dialogisierungsdaten erfolgt bei der programmtechnischen Lösung im Dialogbetrieb zwischen den beteiligten Rechnern auf der Basis eines gemeinsam festgelegten Protokolls. Technisch relativ schwierig zu realisieren war das technische Konzept eines synchronisierten Update-Verfahrens, bei dem die Verarbeitungsergebnisse gleichzeitig in die Versicherungskonten der beteiligten Versicherungsträger und den Stammsatzbestand der DSRV übernommen werden (zum Beispiel wenn zwei Stellen bei der Online-Vergabe einer Versicherungsnummer und drei Stellen beim Wechsel der Kontoführung im Dialog beteiligt sind).
Sofern es bei einem der Partner zu einem Abbruch in der Verarbeitung kommt, müssen alle bereits erfolgten „Zwischenupdates“ bei den am Dialogisierungsverfahren beteiligten Stellen zurückgesetzt werden (so genanntes Rollback).

Serviceorientierter Datenaustausch mit RV (STAR)

Im Verfahren STAR wird mit XML-basierter Kommunikation im eXTra-Standard zwischen den RV-Trägern und der DSRV kommuniziert. Es erfolgt ein Austausch von Datenpakten, die Datensätze zu diversen IT-Verfahren der DSRV enthalten. Jedes von der DSRV empfangene Datenpaket enthält maximal 10 Datensätze. Die über STAR auszutauschenden Datensätze sind von der Fachgruppe Datenaustausch (FGDTTH) abschließend definiert.

Der Geschäftsprozess basiert auf der gesetzlichen Grundlage § 145 (1) SGB VI – Aufgaben der Datenstelle der Rentenversicherung

- Datenübernahme von den RV-Trägern
- Datenverteilung an die Fachverfahren

Der Service hat mehrere Aufgaben:

1. Daten vom RV-Träger entgegennehmen und für servicenehmende DSRV-Fachverfahren bereitstellen
2. Eingangsdatensätze statistisch erfassen, um sie im Statusverfolger sichtbar zu machen.
3. Datensätze mit unzulässigen SK-KE-Kombinationen abweisen.
4. Die Ausgangsdatensätze von servicenehmenden DSRV-Fachverfahren übernehmen und an die RV-Träger versenden.
5. Die Datensätze im Ein - und Ausgang archivieren und nach 90 Tagen löschen

ZUSAMMENFASSUNG

- Ausgehend vom Zweck des Versicherungskontos wurde in Kapitel 8 beschrieben, wie die Daten des Versicherungskontos aktuell gehalten werden. Sie haben dazu gesehen, welche Stellen dabei eine Rolle spielen und haben das DEÜV-Verfahren als wichtigstes Beispiel für den maschinellen Datenaustausch kennengelernt. Sie kennen nun das Verfahren, wie die Daten innerhalb der Rentenversicherung ausgetauscht werden und wissen, dass die Dialogisierung nicht nur Geschwindigkeitsvorteile bringt, sondern insbesondere die Beratung unserer Versicherten unterstützt.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

35. Welche Arten von Fehlerprüfungen kennen Sie?

36. Mit welchem Datensatz ist die Eingabekontrolle realisiert?

37. Über welche zentralen Einrichtungen erfolgt das Meldeverfahren?

38. Was ist der Kern des Themas Dialogisierung des Datenaustausches zwischen den Trägern der gesetzlichen Rentenversicherung?

39. Welche Auskünfte können im Dialog angefordert werden?

9. Geschäftsprozesse und Verarbeitung der Versicherungskonten

LERNZIELE

- Sie kennen die Grundstruktur der Verarbeitung des Versicherungskontos
- Sie können erklären, was unter Geschäftsprozessen zu verstehen ist und wissen wie diese beschrieben werden.
- Sie können die verschiedenen Verarbeitungsformen erklären und die erforderlichen Eingaben und Ergebnisse nennen.
- Sie können die Vorteile einer maschinellen Vorgangsbearbeitung beschreiben und einige der derzeit eingesetzten Workflow-Systeme in der Rentenversicherung benennen.

Sinn und Zweck des Versicherungskontos ist es letztendlich, möglichst ohne weitere zusätzliche Arbeiten, die Versicherung durchzuführen, Leistungen festzustellen und zu erbringen sowie Auskünfte zu erteilen.

Die in den vorherigen Kapiteln dargestellten Verfahren, von der Vergabe der Versicherungsnummer über den Kontenaustausch bis hin zur Kontenaktualisierung, haben daher vor allem vorbereitende Funktionen, um die vorgenannten gesetzlich vorgeschriebenen Aufgaben möglichst effizient, wirtschaftlich und vor allem im Interesse der Versicherten auch korrekt sowie in angemessener Zeit erfüllen zu können.

Die Verarbeitung richtet sich dabei an den Geschäftsprozessen der Rentenversicherung (zum Beispiel Altersrente berechnen) und deren Produkten (zum Beispiel Rentenbescheid, Zahlungsanweisung) aus. Im Sinne einer modernen Verwaltung und den Erfordernissen, die sich an das Rentenversicherungssystem rvDialog stellen, spielt dabei der strukturierte Ablauf in Form eines elektronischen Workflows eine bedeutende Rolle.

9.1 Grundstruktur der Verarbeitung des Versicherungskontos

Ebenso vielfältig und umfangreich, wie die gesetzlichen Aufgaben sind auch die maschinellen Verarbeitungsroutinen des Programmsystems. Ein erster Überblick ergibt sich aus der folgenden Zusammenstellung der gebräuchlichsten Verarbeitungsmöglichkeiten mit den dazu erforderlichen Eingaben und deren Ergebnissen.

Anlässe der Verarbeitung

Die Anlässe und Auslöser für die Verarbeitung der Versicherungskonten können zunächst in die auch seitens der Organisationsformen der Versicherungsträger klassischen Bereiche

- **Beitrag** (zum Beispiel Beitragseinzug, Feststellung von Zeiten oder Beitragserstattung),

- **Rehabilitation** (zum Beispiel Bewilligung der Leistung, Bewilligung des Übergangsgeldes oder Abrechnung)

  und

- **Rente** (zum Beispiel Inlandsrenten, Auslands- und Vertragsrenten, Bonus oder Malus, Vergleichsberechnungen, Einkommensanrechnung, knappschaftliche Besonderheiten).

aufgeteilt werden. Ergänzend hinzukommen die weiteren Aufgaben wie

- **Auskünfte** aus dem Konto (zum Beispiel rentenartbezogene Auskunft oder Ehezeitauskunft)

  sowie

- **sonstige Verarbeitungen** (zum Beispiel Rentennachbehandlung, Erstattungsverfahren oder Schadenersatzverfahren, ausgelöst durch rveServices).

Die sonstigen Verarbeitungsverfahren haben ihre Grundlage in bereits festgestellten Leistungen. Sie dienen in der Regel der Zahlung einmaliger oder laufender Leistungen oder Abrechnungen mit anderen Stellen.

Die erforderlichen Sachbearbeiter-Eingaben beziehungsweise Arbeitsaufträge sind ebenso unterschiedlich und vielfältig wie die Aufgaben selbst. Ein komplettes Konto vorausgesetzt, brauchen in der Regel jedoch immer nur der Auftrag selbst, ergänzende Leistungsdaten (beispielsweise Beginn- und Ende-Datum der Leistung), Anschriften, Kontendaten sowie statistische Daten angegeben werden.

Auslöser für Verarbeitungen

Die Auslöser für die einzelnen Verarbeitungen sind dabei unterschiedlich. Wir unterscheiden grundsätzlich drei Arten, nämlich:

- **Manueller** Auftrag
  Insbesondere im Rahmen der Bewilligung und Erbringung von Leistungen sowie der erforderlichen Nachbehandlungen erfolgt der Auslöser manuell durch die Sachbearbeitung. Dies kann vorgenommen werden durch die Eingabe von Arbeitsaufträgen, die Speicherung von Auftragssatzarten zusammen mit anderen Informationen oder die Speicherung von Daten, die maschinelle Folgeverarbeitungen auslösen.

- **Maschinelle** Auslösung beziehungsweise Folgeverarbeitung
  Ebenso wie bei der manuellen Einspeicherung können auch maschinell übermittelte Daten Folgeverarbeitungen auslösen. Dies gilt beispielsweise nach der Leistungsbewilligung im Reha-Bereich, wo die maschinelle Entlassungsanzeige die Endabrechnung des Übergangsgeldes, der Zuzahlung sowie der Sachleistungen auslöst.

- **Turnusmäßige** beziehungsweise besondere maschinelle Verarbeitung
  Teilweise können die Verfahren auch völlig maschinell ablaufen. Dies erfolgt im Rahmen der maschinellen Terminverfolgung (zum Beispiel Einstellung von Zeitrenten, Kinderwegfälle) oder sachbezogenen Verarbeitungsläufen (monatlicher Beitragseinzug, Einkommensüberprüfung, statistische Meldungen). Besondere Verarbeitungsläufe gehen häufig auf geänderte gesetzliche Vorschriften oder höchstrichterliche Rechtsprechungen zurück, wobei für bestimmte Personenkreise neue Leistungen festgesetzt beziehungsweise bestehende Leistungen überprüft werden.

Während die zuerst genannten Aufträge sich immer nur auf eine konkrete Versicherungsnummer und damit ein Versicherungskonto beziehen, betrifft die turnusmäßige Verarbeitung im Prinzip die Verarbeitung des gesamten Kontenbestandes nach bestimmten Kriterien. Die Sachbearbeitung wird dabei bei Bedarf lediglich durch die Vorlage der maschinellen Ergebnisse, zum Beispiel Zahlungsaufträge, beteiligt.

Ergebnisse

Die Ergebnisse der Berechnung und Feststellung der Leistung, des Beitragsverfahrens sowie der Auskünfte sind zumeist Verwaltungsakte. Sie werden daher sowohl dem Versicherten gegenüber als grundsätzlich auch in der Akte (für Prüfungs- und Rechtsmittelzwecke) auf **Papier** dokumentiert. Zukünftig wird die elektronische Archivierung dieser Belege und Bescheide das Papier mehr und mehr ersetzen. Mit der daraus resultierenden elektronischen Akte beschäftigen wir uns in Kapitel 9.4.

Die Rentenleistungen, Beitragserstattungen, Abrechnungen mit anderen Stellen sowie sonstige Auszahlungen erfolgen grundsätzlich über **Zahlungsanweisungen** oder **Zahlungsaufträge** (ZA) an den Renten Service der Deutschen Post AG. Die Daten werden maschinell aus dem Konto beziehungsweise den Berechnungsergebnissen gewonnen und dem Renten Service ebenfalls maschinell übermittelt. Die sonstigen Zahlungen, insbesondere die Reha-Barleistungen (Übergangsgelder, Sachleistungen, Pflegekosten) werden über das Bankzahlverfahren ausbezahlt. Auch hier erfolgt die Bankanweisung über das für den gesamten Bankverkehr gültige Verfahren des „Beleglosen Datenträgeraustausches“. In diesem Rahmen werden die Daten der Giroüberweisungsträger beziehungsweise Bankabbuchungsbelege in normierte Datensätze abgelegt und den Banken elektronisch übermittelt. Die Abrechnungen, Verbuchungen und so weiter müssen hier hausintern erfolgen.

Mit der Einführung eines neuen Überweisungs- und Lastschriftverfahrens im Europäischen Zahlungsraum zum 1.1.2008 (SEPA – Single European Payments Area) wurde der elektronische Zahlungsverkehr weiter gestärkt. Damit verbunden sind die Ablösung der bisherigen Kontonummer und Bankleitzahl durch BIC (Bank Identifier Code) und IBAN (International Bank Account Number) ebenso wie das neue SEPA-Lastschriftverfahren. Zwischenzeitlich haben BIC und IBAN ihren Eingang bereits in das Rentenzahlverfahren und die Vordrucke und Formulare gefunden.

Alle **maschinellen Ergebnisdaten** werden im Versicherungskonto abgelegt. Auf diese kann dann bei Folgeleistungen oder im Rahmen der Nachbehandlung zurückgegriffen werden.

In diesem Rahmen werden auch eine Vielzahl von Daten gehalten und gespeichert, die rein statistischer Natur sind. Dies folgt aus der Verpflichtung nach der Allgemeinen Verwaltungsvorschrift über die Statistik in der Rentenversicherung (RSVwV), nach der die Rentenversicherungsträger verpflichtet sind, sowohl über die Konteninhalte, die Versicherung als auch über Leistungen umfangreiche **statistische Basisdaten** zu liefern. Diese Datensätze werden maschinell aus den Konten aufgebaut und in turnusmäßigen Abständen (monatlich, jährlich) zur Auswertung an die Deutsche Rentenversicherung Bund und teilweise auch an statistische Landesämter beziehungsweise den Bund geliefert. Diese statistischen Auswertungen dienen nicht nur der internen Betriebssteuerung der Versicherungsträger, sondern sind auch Grundlage politischer Entscheidungen im Gesetzgebungsverfahren sowie dem Finanzausgleich.

9.2 Geschäftsprozesse

Die einzelnen Verarbeitungsaufträge lernen Sie im Rahmen ihrer praktischen Ausbildung kennen. Jede Verarbeitung erfüllt dabei spezielle Aufgaben bei der Erledigung eines Geschäftsprozesses und der Erzielung des gewünschten Ergebnisses. Auf dieses Thema sowie die Darstellung und Steuerung von Geschäftsprozessen im Rahmen der Organisationsplanung und der IT-Umsetzung soll im Folgenden etwas genauer eingegangen werden.

Geschäftsprozess und Vorgang

Organisatorisch betrachtet beschreibt ein **Geschäftsprozess** eine Folge von Einzeltätigkeiten, die schrittweise ausgeführt werden, um ein geschäftliches oder betriebliches Ziel – zum Beispiel die Erstellung eines Rentenbescheides – zu erreichen. Dabei kann der Prozess selbst auch öfter durchlaufen werden. Ein Geschäftsprozess kann Teil eines anderen Geschäftsprozesses sein oder andere Geschäftsprozesse enthalten beziehungsweise diese anstoßen. Geschäftsprozesse gehen oft über Abteilungen und Betriebsgrenzen hinweg und gehören zur Ablauforganisation eines Unternehmens oder einer Behörde.

Bei den Einzelschritten eines Prozesses kann es sich um manuelle Tätigkeiten handeln (zum Beispiel ein Telefonat, Datenerhebung- und -erfassung, Prüftätigkeiten und so weiter) oder um vollmaschinelle Verfahren wie etwa die eigentliche Rentenberechnung. Anders als in der Fertigung sind heutzutage im Verwaltungsbereich die meisten Arbeitsschritte zumindest
IT-unterstützt.

Der Geschäftsprozess als solches ist eine abstrakte Beschreibung. Ein **Vorgang** hingegen ist die konkrete Ausprägung eines Geschäftsprozesses, der durch spezifische Bearbeiter, die konkret verwendeten Dokumente und Daten, bestimmte Zeitpunkte und durch das erzielte Ergebnis definiert ist.

Geschäftsprozessmodellierung

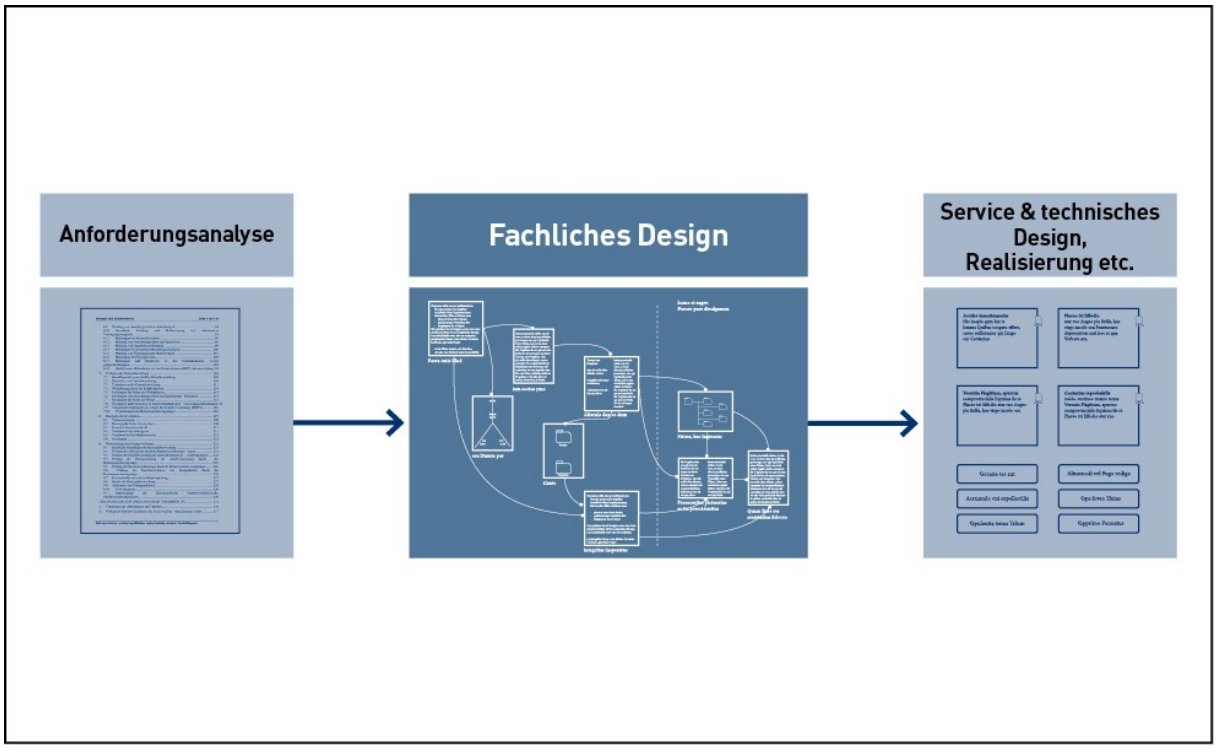
Zur Beschreibung und Darstellung von Geschäftsprozessen haben sich gewisse Standards herausgebildet. Man spricht in diesem Zusammenhang auch von Geschäftsprozessmodellierung.

Im Rahmen des Integrationsprogramm IPibiza ging man davon aus, dass für ein RV-System etwa 180 bis 200 unterschiedliche Geschäftsprozesse erstellt werden müssen. Die Aufgabe besteht dabei darin, den benannten Geschäftsprozess aus den beiden bestehenden Systemen zu analysieren, zu vereinheitlichen, ihn zu beschreiben und im neuen Zielsystem technisch umzusetzen.

Hierfür wurde in einem ersten Schritt eine Ist-Analyse der Geschäftsprozesse vorgenommen. Danach war zu prüfen, inwieweit eine Vereinheitlichung möglich wäre und ob ggf. notwendige Abweichungen durch Steuerungsoptionen im Prozessablauf realisiert werden könnten.
Anschließend sollte die fachliche Modellierung des Geschäftsprozesses als Grundlage für die Umsetzung im neuen Zielsystem durchgeführt werden. Auf der Grundlage der fachlichen Modellierung wurde anschließend das technische Geschäftsprozess-, Service- und Datenmodell erstellt und die technische Umsetzung des Geschäftsprozesses in die neue Architektur vorgenommen. Im Laufe des Projekts IPibiza wurde die Vorgehensweise zur Vereinheitlichung des Programmsystems allerdings geändert. Auf Grund der Komplexität der Programme wurde beschlossen, vor der Schaffung einheitlicher, optimierter und automatisierter Geschäftsprozesse im ersten Schritt in einem Migrationsprojekt und im Integrationsprogramm IPibiza zunächst die Referenzversion des GRVS an die technischen Anforderungen der DRV Bund anzupassen und um die von der DRV Bund zwingend benötigten Funktionalitäten zu erweitern.

Die fachliche Beschreibung des Geschäftsprozesses steht dabei immer noch im Mittelpunkt. Sie beginnt mit einer Analyse der Anforderungen an den Geschäftsprozess und dessen Rahmenbedingungen. Dieses fachliche Design bestimmt die anschließende technische Umsetzung.

Abbildung 8: Fachliches Design von Geschäftsprozessen



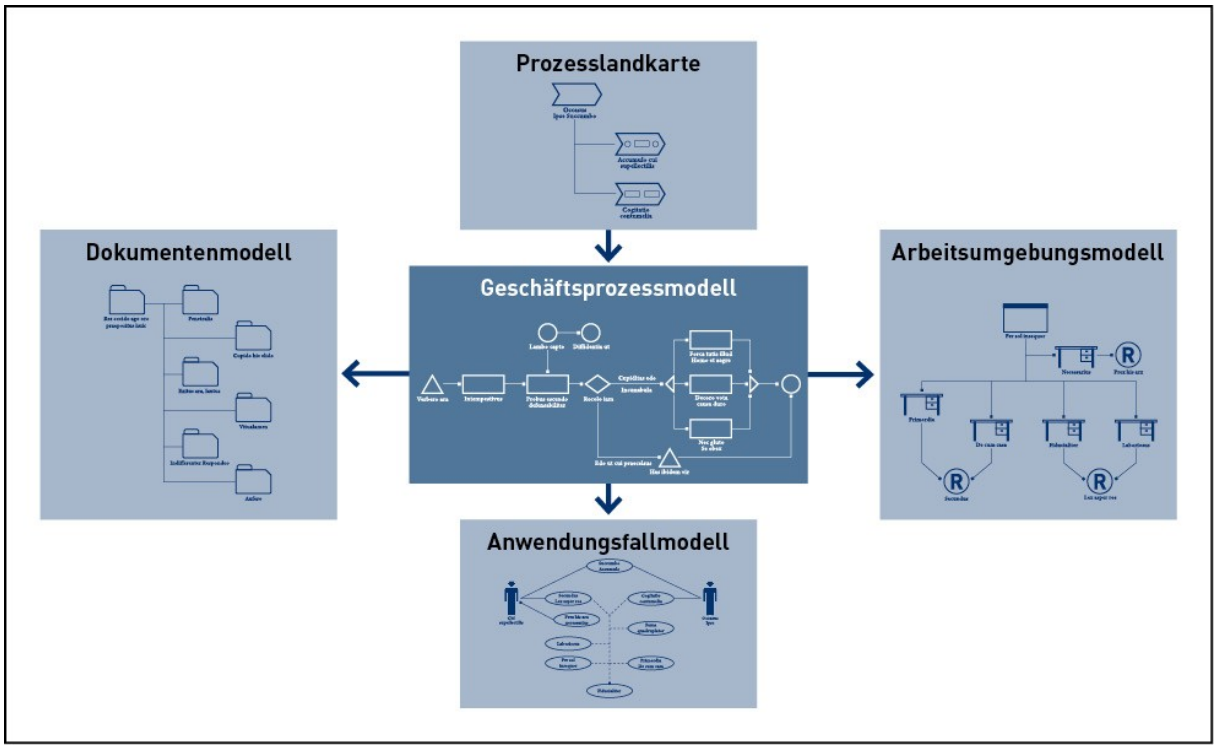
Die Spezifikation des Geschäftsprozesses besteht in der Regel aus einer Reihe von Dokumenten und Modellen. Oftmals werden in Projekten in der Phase der Modellierung unterschiedliche Werkzeuge wie Textverarbeitung und Grafikprogramme eingesetzt.

Modellierungstools

Neben dem notwendigen Fachwissen (Prozesskennende) benötigt man grafische Darstellungen zur Geschäftsprozessbeschreibung und nutzt hierfür sogenannte Modellierungstools. Typische Vertreter sind Programme wie ARIS und ADONIS. Deren Output lässt sich im Idealfall über entsprechende Modellierungssprachen - zum Beispiel der Unified Modeling Language (UML) - auch direkt an die Programmentwicklung weitergeben. Mit der Geschäftsprozessmodellierung und ihrer grafischen Darstellung trägt man zugleich der Tatsache Rechnung, dass die IT-Systeme sehr groß und umfänglich sind und daher Teamarbeit und Kommunikation notwendig ist, um sie vollständig zu beschreiben und umzusetzen. Nicht nur Programmierer, auch Manager, Fachbereich und Kunden sind in den Entwicklungsprozess involviert. Somit ist eine gemeinsame, verständliche Sprache notwendig. Gleichzeitig entsteht eine detaillierte Dokumentation. Dies trägt der Tatsache Rechnung, dass die natürliche Sprache manchmal mehrdeutig und unpräzise ist, während Programmiersprachen zwar präzise, aber nicht für alle (zum Beispiel Fachbereiche) verständlich sind.
Die graphische Modellierung mit UML füllt diese Lücke aus. UML ist graphisch und objektorientiert sowie unabhängig von den verwendeten Entwicklungsstandards und -methoden. Sie beinhaltet insgesamt neun Diagrammarten, um die verschiedenen Aspekte von Softwaresystemen und deren Entwicklung widerzuspiegeln.

Die **Prozesslandkarte** dient der Übersicht und dem Zusammenspiel der Geschäftsprozesse untereinander. Im Mittelpunkt steht das eigentliche Geschäftsprozessmodell zur detaillierten Darstellung von Abläufen. Die grafische Aufbereitung erfolgt in einem **Aktivitätendiagramm** (oder Ablaufdiagramm**)** mit Einzelfunktionen (Rechtecke), Ablaufpfeilen, Verzweigungen (Rauten) und weiteren Symbolen. Hiervon ausgehend werden aus den fachlichen Prozessmodellen die organisatorischen Anforderungen, Anwendungsfallbeschreibungen, Entwürfe der grafischen Benutzeroberfläche und Testfälle abgeleitet und dokumentiert.

Abbildung 9: Beispiele für UML-Diagramme und deren Zusammenspiel



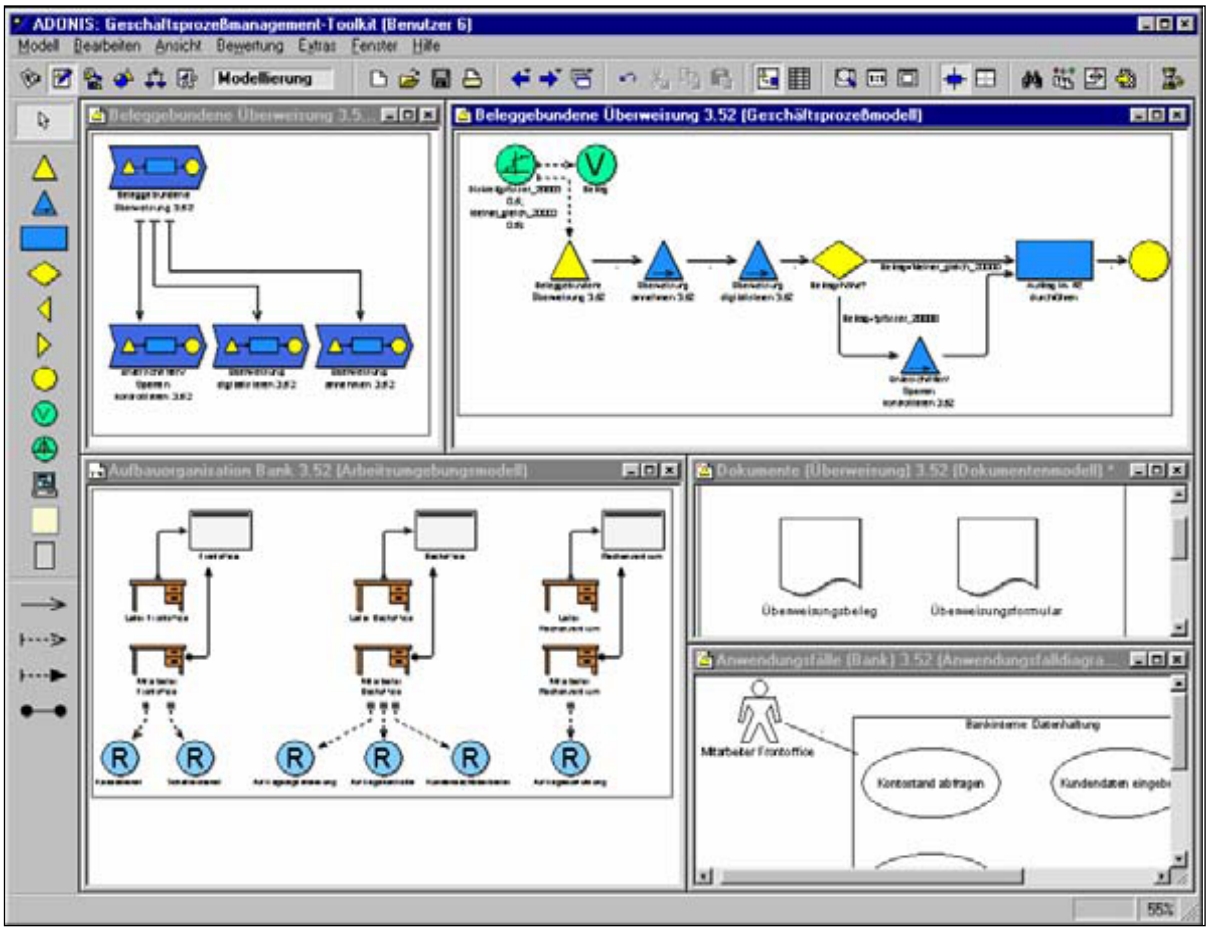
Das **Anwendungsfalldiagramm** dient zur Darstellung der Interaktion zwischen einem Benutzer und einem System. Das Arbeitsumgebungsmodell stellt die benötigten Organisationsstrukturen dar. Im Dokumentenmodell werden die in Geschäftsprozessmodellen verwendeten Dokumente und Informationen aufgezeigt. Ein **Datenmodell** schließlich beschreibt die zur Abarbeitung des Geschäftsprozesses notwendigen Eingabedaten beziehungsweise die erzeugten Ergebnisse.

Die zur Geschäftsprozessmodellierung angebotenen Programme bieten darüber hinaus zahlreiche weitere Funktionen zur Analyse (Personalaufwand, Kosten) und Simulation (zur Optimierung der Prozesse). Außerdem lassen sie sich mit den Entwicklungswerkzeugen der Programmierung verknüpfen, um die fachlichen Modelle in technische Modelle und schlussendlich funktionierende Systeme umzusetzen.

Prozesssteuerung

Während bei den heutigen RV-Systemen die Steuerung des Prozesses noch weitgehend bei der Sachbearbeitung liegt – durch Eingabe von Daten und/ oder Arbeitsanweisungen – übernimmt mit steigendem Automatisierungsgrad die Maschine auch wesentliche Steuerungsfunktionen. Sie sorgt dafür, dass der Mensch nur noch dort eingeschaltet wird, wo zusätzliche Informationen oder eine Freigabe benötigt werden. Ansonsten wird der Geschäftsprozess durch den Rechner verwaltet und gesteuert. Im nächsten Kapitel wollen wir uns daher solche bereits heute bestehende Workflow-Systeme in der Rentenversicherung ansehen.

Abbildung 10: Beispiel für ein Modellierungstool: ADONIS mit grafischer Darstellung



9.3 Der elektronische Workflow

Wenn vom Technologiewandel in der Deutschen Rentenversicherung die Rede ist, denkt man neben der Neugestaltung der Kundenschnittstellen durch Online-Services (siehe auch nächstes Kapitel) vor allem an Automatisierung und Digitalisierung.

Es zeichnet sich ab, dass sich elektronische Arbeitsabläufe (**Workflows**) auch im Kerngeschäft und in wesentlichen Unterstützungsprozessen der Deutschen Rentenversicherung durchsetzen werden. Mittelfristig werden ganze Geschäftsprozesse oder Geschäftsprozessketten im Rahmen von elektronischen Workflow-Systemen realisiert werden. Dabei erfolgt eine Automatisierung beziehungsweise Teilautomatisierung der Einzelprozesse. Voraussetzungen für den elektronischen Workflow sind die digitale Archivierung von Vorgängen in einem Dokumentenmanagementsystem (DMS) und die elektronische Akte.

Durch die Automatisierung der Kernanwendung sinkt der Zeitanteil menschlicher Arbeit bei der unmittelbaren Vorgangsbearbeitung (Ermittlung, Prüfung, Berechnung und so weiter). Dies erfolgt, indem die Geschäftsprozesse neu modelliert und bestimmte Arbeitsschritte, die bislang zur direkten Vorgangsbearbeitung gehörten, durch das IT-System übernommen werden.

Der Unterschied zur bisherigen IT-Unterstützung besteht darin, dass nicht nur einzelne Arbeitsschritte automatisiert erfolgen, sondern der Workflow die Prozesssteuerung übernimmt. Die Prozesssteuerung im IT-System legt fest, welche Arbeitsschritte (Ermittlungen, Prüfungen und so weiter) in welcher Abfolge zur Erfüllung notwendig sind und organisiert diese Schritte (Einleitung, Überwachung, Prüfung, Rückmeldung, Zusammenführung).

Die Sachbearbeitung bearbeitet in der Regel Einzelaufgaben, die nicht zwingend in einem inhaltlichen beziehungsweise organisatorischen Zusammenhang zum Ergebnis (zum Beispiel Bescheid) stehen, da dieser Zusammenhang vom Workflow hergestellt wird. Das Wissen über den Gesamtvorgang ist für viele Aufgaben somit nicht unbedingt notwendig und kann - im Unterschied zu heute - auch zeitgleich mehreren Akteuren an verschiedenen Stellen zur Verfügung gestellt werden.

Vorteile/ Nachteile

Die Rentenversicherungsträger haben erhebliche finanzielle Investitionen getätigt und personelle Aufwendungen zur Einführung von elektronischen Antragsverfahren und zur Implementierung der Online-Dienste erbracht. Ziel dieser Initiativen war es vor allem bürgerfreundliche Angebote zur Verfügung zu stellen, die dem aktuellen technischen Standard entsprechen. Die Wirtschaftlichkeit solcher Investitionen – nach dem SGB IV sind die Rentenversicherungsträger zum wirtschaftlichen Handeln verpflichtet – lässt sich jedoch nur dann begründen, wenn die elektronischen Anträge auch beim Rentenversicherungsträger medienbruchfrei in die Kernsysteme einlaufen und dort eine maschinelle Vorgangsbearbeitung anstoßen. Nur so lassen sich die Einspar- und Rationalisierungspotenziale von Workflowsystemen realisieren.

Mit der Einführung von Workflowsystemen in der Rentenversicherung werden allgemein folgende Ziele verfolgt:

- Verbesserung der Prozessqualität durch maschinelle Steuerung und Unterstützung der Prozesse,

- Schnellere und zuverlässigere Bearbeitung von Anträgen durch Verkürzung der Transport- und Liegezeiten,

- Vermeidung von Medienbrüchen von der maschinellen Antragserfassung bis zur maschinellen Bescheiderteilung und Zustellung,

- Erhöhung der Informationsverfügbarkeit durch Zugriffsmöglichkeit auf die Akten und Daten an jedem Ort und zu jeder Zeit,

- Kontrollierter Fluss von Daten und Dokumenten (Daten und Dokumente werden so zusammengeführt und gesteuert, dass sie immer zum richtigen Zeitpunkt am richtigen Ort verfügbar sind),

- Erhöhung der Transparenz der Prozesse (Statusermittlung, Dokumentation von Entscheidungen),

- Verbesserung der Datenqualität infolge durchgängiger maschineller Plausibilitäts- und Zusammenhangsprüfungen während des Gesamtprozesses und letztlich

- Reduzierung der Verwaltungs- und Verfahrenskosten.

Die Rentenversicherungsträger haben sich daher für die Einführung solcher Anwendungen entschieden. Einige der zurzeit eingesetzten Workflowsysteme sollen nun kurz vorgestellt werden.

Zentrale Zulagenstelle für Altersvermögen (ZfA)

Mit dem Altersvermögensgesetz (AVmG) wurden die Aufgaben der Zentralen Stelle im Sinne des § 81 EStG der damaligen Bundesversicherungsanstalt für Angestellte (BfA), der Vorläuferbehörde der Deutschen Rentenversicherung Bund übertragen. Mit dem AVmG wird der Aufbau einer zusätzlichen Altersvorsorge in der betrieblichen oder in der privaten Vorsorge steuerlich und durch Zulagen gefördert.
Die ZfA hat ihren Sitz in Brandenburg an der Havel. Sie nimmt Aufgaben der Finanzverwaltung wahr und unterliegt der Fachaufsicht des Bundeszentralamtes für Steuern (BZSt). Ihre wesentlichen Aufgaben sind:

- die jährlich wiederkehrende Feststellung, in welcher Höhe ein Zulagenanspruch (Grund- und Kinderzulage) und von welchem Zeitpunkt an dieser Anspruch besteht,
- die Auszahlung zugunsten des Zulageberechtigten an den Anbieter zur Verbuchung auf dem Altersvorsorgevertrag,
- die Rückabwicklung zu Unrecht gezahlter Zulagen,
- das Verfahren bei Verwendung eines Kapitalteilbetrages aus einem Altersvorsorgevertrag zum Erwerb oder Herstellung von selbstgenutzem Wohneigentum
  und
- den Datenabgleich mit den RV-Trägern, der Bundesagentur für Arbeit, den Meldebehörden, den Familienkassen und Finanzämtern zur Überprüfung der Zulage und des Sonderausgabenabzugs. Die ZfA ist berechtigt, die ihr übermittelten Daten mit den Angaben im Zulagenantrag abzugleichen.

Die ZfA bedient sich zur Erledigung dieser Aufgaben der elektronischen Akte und eines automatisierten Vorgangssystems mit Namen zusy (Zulagensystem). Das Projekt ist ein vollelektronisches Verfahren zur Berechnung, Auszahlung und Überprüfung der zulagengeförderten Altersvorsorge. In einem Dokumentenmanagementsystem werden eingehende Poststücke digitalisiert und elektronisch bearbeitet, die Daten der Anbieter (Versicherungen, Banken etc.) werden elektronisch erfasst und führen zum ebenfalls maschinell durchgeführten Auszahlverfahren. Für den Datenabgleich mit Rentenversicherungsträgern, Finanzämtern etc. ist eine elektronische Kommunikation mit bis zu 18.000 Stellen erforderlich.

Der ZfA wurden weitere Aufgaben im Zusammenhang mit dem Rentenbezugsmitteilungsverfahren (rebsy) und dem maschinellen Anfrageverfahren zur Erlangung der Identifikationsnummer nach § 139b AO (MAV) übertragen.

Minijob-Zentrale

Minijobs sind bei der Minijob-Zentrale, die bei der Deutschen Rentenversicherung Knappschaft Bahn See eingerichtet ist, zu melden. Die Aufgaben der Minijob-Zentrale sind dabei vielfältig und facettenreich.

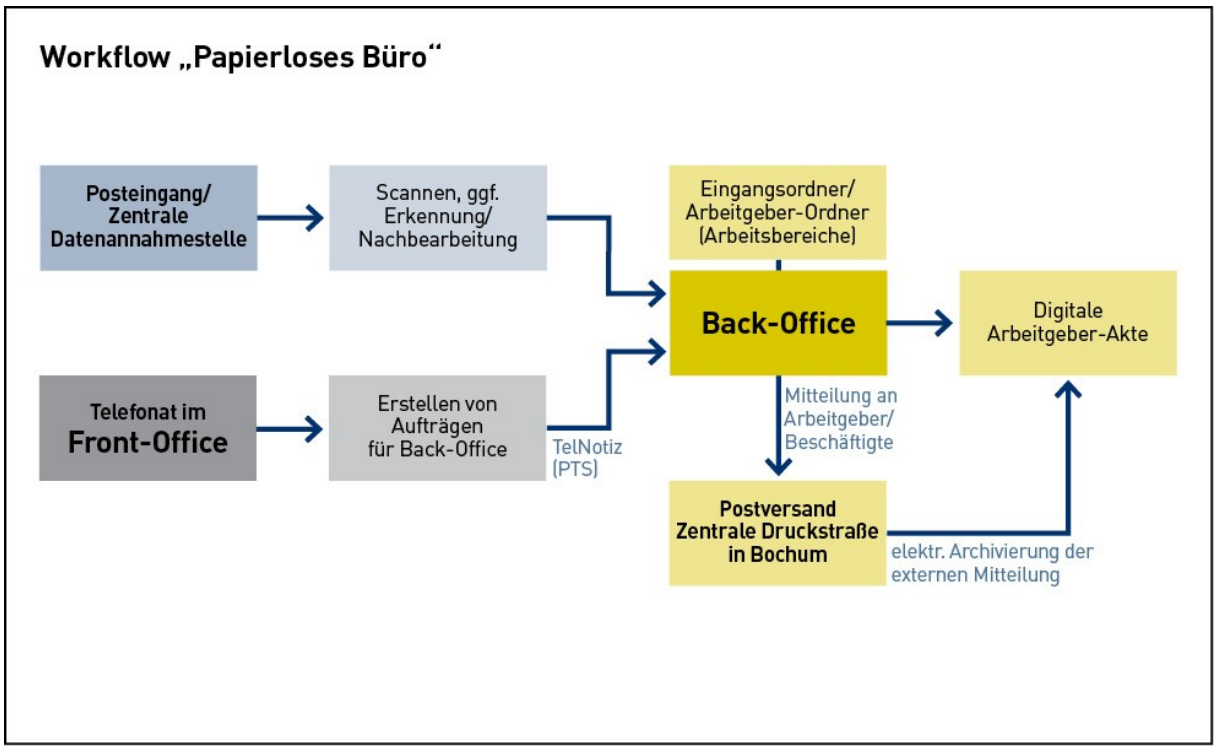
Sie umfassen

- das Meldeverfahren und den Einzug von Pauschalabgaben bei allen geringfügig Beschäftigten,
- die Durchführung des Haushaltsscheckverfahrens,
- die Weiterleitung der Beiträge an die zuständigen Stellen; das heißt, die tägliche Weiterleitung der Rentenversicherungsbeiträge sowie die gleichmäßige Aufteilung der Beiträge für die Krankenversicherung über den Risikostrukturausgleich,
- die Prüfung der Versicherungspflicht beziehungsweise der Versicherungsfreiheit,
- die Überwachung der Zahlungseingänge,
- die Bearbeitung von Rückstandsfällen und Insolvenzfällen,
- die Durchführung der Lohnfortzahlungsversicherung nach dem Lohnfortzahlungsgesetz für Arbeitgeber mit bis zu maximal 30 Beschäftigten,
- den Einzug der Pauschalsteuer in Höhe von 2%

  sowie

- die Beratung der Arbeitgeber und der Beschäftigten.

Abbildung 11: Workflow in der Minijob-Zentrale



Ein wichtiges Anliegen der Deutschen Rentenversicherung Knappschaft-Bahn-See ist seit Übernahme der neuen Aufgabe die Vereinfachung der Verwaltungsvorgänge und damit die Erleichterung der Arbeit für die Arbeitgeber.

In Essen befindet sich das Finanz- und Logistikzentrum der Minijob-Zentrale. Hier ist unter anderem der Post- und Scheckeingang angesiedelt. Zur Bewältigung des großen Schriftverkehrs und für eine hohe Bearbeitungseffizienz wird in der Minijob-Zentrale die Aktenführung weitestgehend im Rahmen des Dokumentenmanagements digital durchgeführt. Zu Spitzenzeiten treffen täglich bis zu 70.000 Dokumente ein. Eingehende Post wird in einer zentralen Datenannahmestelle geöffnet, gescannt, gegebenenfalls nachbearbeitet und dem Back-Office zielgerichtet in jederzeit einsehbaren, digitalen Arbeitgeberordnern zugestellt. Eingehende Telefonate können durch das Front-Office ebenfalls zielgerichtet dem zuständigen Back-Office in Form von digitalen Arbeitsaufträgen zugeteilt werden.

elektronischer Workflow

Ein elektronischer Workflow und die Abbildung im RV-System ist auch ein wesentlicher Bestandteil des Programmsystems rvDialog. Mit den Veränderungen, die dieser Technologiewandel in die Arbeitswelt bringt, hat sich auch das Projekt „Arbeitsorganisatorische Gestaltungsoptionen bei der Weiterentwicklung der IT-Systeme der Deutschen Rentenversicherung“ (ARGONIT) beschäftigt. Es hatte den Auftrag, Informationen über die mit dem Technologiewandel verbundenen Veränderungsprozesse zu gewinnen und Gestaltungsoptionen zur Steuerung der Veränderungen im Interesse der Kunden, des Unternehmens und der Beschäftigten zu erkennen. Interessierte Leserinnen und Leser werden für weitere Erläuterungen auf den ARGONIT-Abschlussbericht verwiesen (FAO 1/2009, TOP 18).

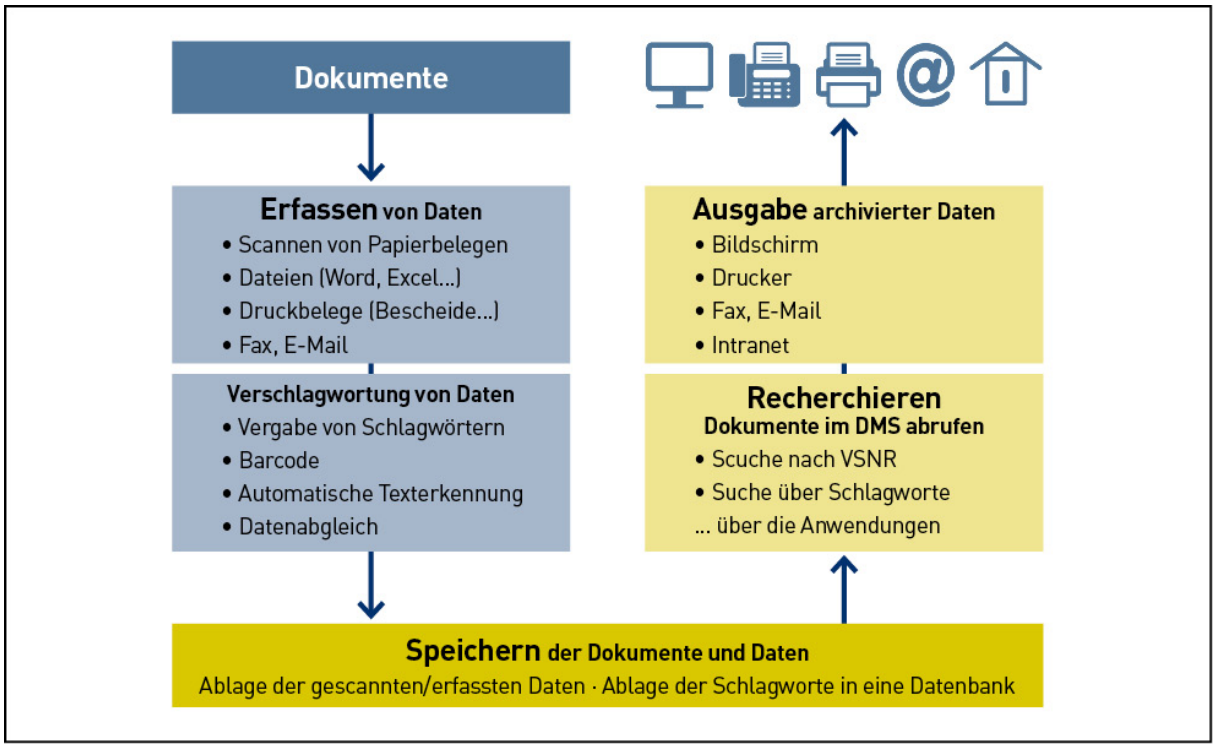
9.4 Digitales Akten-Management als Voraussetzung für Workflows

Ein revisionssicheres Langzeitarchiv auf elektronischer Basis ist Voraussetzung für die weitere Automatisierung der Aktenbearbeitung. Es dient allen aktuellen und künftigen Fachanwendungen als Basis für eine vollständige elektronische Vorgangsbearbeitung.

Die Versicherungsakte enthält alle nicht maschinell gespeicherten Unterlagen und Belege. Bislang hat die Verwaltung dieser Akten große personelle und räumliche Kapazitäten gebunden und war medientypischen Nachteilen unterworfen: Eine Akte existiert nur einmal und muss manuell transportiert und geordnet werden.

Digitale Akten

Abbildung 12: Funktionsübersicht „Elektronische Archivierung“



Unter Digitalisierung versteht man in diesem Zusammenhang die Archivierung von Akten und Dokumenten in elektronischer Form auf der Basis eines Dokumentenmanagementsystems (DMS). Dokumente können direkt aus der Fachanwendung oder aus einem angeschlossenen Erfassungssystem archiviert werden. Auch die Übernahme von Daten in elektronischer Form (Druckausgabe von Bescheiden, maschinelle Zahlungsanweisungen) ist möglich. Die Anzeige der Dokumente erfolgt im Fachverfahren oder über einen unabhängigen Recherche-Client. Sämtliche abgelegten Dokumente sind strukturiert und dem jeweiligen Mandanten zugeordnet. Die **digitale Akte** umfasst dabei

- die elektronische Speicherung aller bisher entstandenen Vorgänge im Rahmen einer Einmalaktion unter Einsatz der qualifizierten elektronischen Signatur,

- die Speicherung neu entstandener archivierungswürdiger Vorgänge in der eigenen Digitalisierungsstelle,

- den schnellen Zugriff auf die elektronisch gespeicherten Akten von jedem Arbeitsplatz,
- die Anzeige der Akte in einer einheitlichen Struktur einschließlich Belegungsanzeige,
- die komfortable Recherche mittels eines eigens dafür geschaffenen Recherche-Clients,
- die Vernichtung der körperlichen Akten,
- die Möglichkeit der kompletten Reproduktion der elektronisch gespeicherten Akten (Ausdruck) bei Bedarf.

Vorteile

Als Vorteil der digitalen Akte ist zunächst zu nennen, dass die gesamte Sachbearbeitung schnellen Zugriff auf die elektronisch gespeicherten Akten hat. Der Zeitbedarf für die Anlieferung einer herkömmlichen Akte kann auf Grund der dezentralen Struktur der Sachbearbeitungsbereiche und der bisherigen Zentralarchive bei durchschnittlich mehreren Tagen liegen. Neben der medienbruchfreien Aktenführung entstehen Kostenvorteile durch

- verringerten Personalbedarf für die Verwaltung des Aktenarchivs,
- den Wegfall der Kosten für das Archivgebäude

  sowie

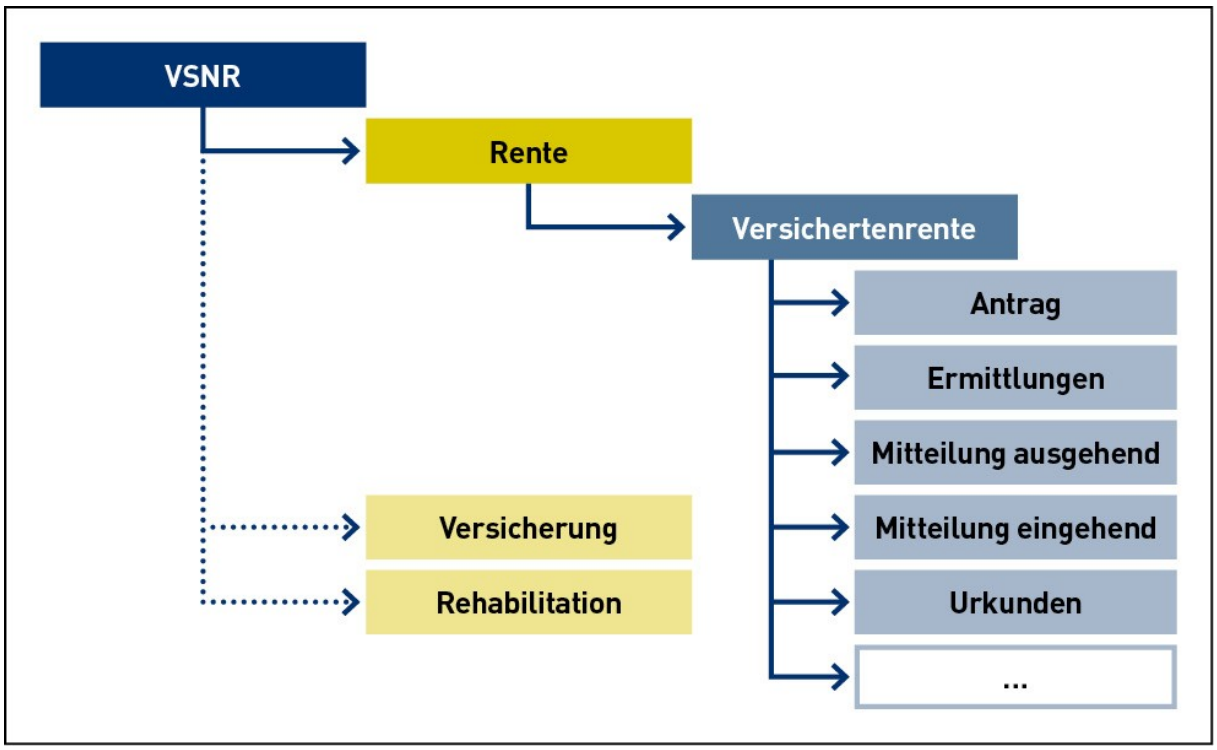
- den Wegfall der Transportkosten.

Inhalt der digitalen Akte in der Rentenversicherung

Der Inhalt der digitalen Akte orientiert sich an der Papierform und gliedert sich entsprechend in die Hauptgruppen Persönliche Daten, Versicherung/ Beitrag, Rente und Rehabilitation. Die nachstehende Abbildung 13: Struktur der digitalen Akte

zeigt exemplarisch, wie die Aktenablage für den Bereich Rente weiter strukturiert werden kann.

Abbildung 13: Struktur der digitalen Akte



Scannen und Abruf

Eine wichtige, aber zeitaufwändige Arbeit bei der Umstellung der Aktenführung ist das erstmalige Digitalisieren der alten Papierakten. Diese müssen sortiert und ggf. strukturiert, von „Ballast“ befreit und für den eigentlichen Scan-Vorgang vorbereitet werden (Entfernen Heftung, Trennblätter etc.). Moderne Hochleistungs-Scanner erfassen die Akten und stellen sie für Nacharbeiten zur Verfügung. Dazu gehört neben der Sichtkontrolle der Erfassung die Verschlagwortung (Indizierung) der Daten und – soweit zur Rechtssicherheit notwendig – die (Massen-) Signatur der elektronischen Akte.

Sobald eine solche elektronische Bearbeitungsbasis gelegt ist, lohnt es sich, die Digitalisierung auch für die laufenden Eingangspost einzusetzen, anschließend für die gezielte Überführung ins elektronische Archiv die Dokumente nach unterschiedlichen Kriterien und/ oder Schlüsselwörtern zu klassifizieren und der jeweiligen elektronischen Akte zuzuordnen. Auch die direkte Übernahme von Daten in elektronischer Form (Druckoutput von Bescheiden, maschinelle Zahlungsanweisungen) sowie von E-Mails oder Fax ist möglich.

Zum Aufruf der elektronischen Akte sowie einzelner zugehöriger Dokumente benötigt man einen Recherche-Client, der die Suche (zum Beispiel nach Versicherungsnummer oder Namen) unterstützt und die elektronische Akte aus dem Archiv abruft. Die grafische Anzeige der Akte und Funktionen wie Blättern, Drucken etc. müssen ebenfalls unterstützt werden. Optimalerweise wird diese Funktionalität im normalen Arbeitsumfeld, beispielsweise dem Programmsystem zur Verfügung gestellt. Bildschirmgrößen von zumeist 21“ oder 24“ sind Standard.

In einem ersten Pilotprojekt im Jahr 2004 wurde das vollständige Aktenarchiv der heutigen DRV Rheinland in ein elektronisches Archiv überführt. Es handelte sich um rund 1,3 Mio. Akten mit einem Gesamtumfang von ca. 120 Mio. Seiten. Seit 2005 werden dort die täglichen Neueingänge im Archiv dem elektronischen Archiv zugeführt. Die anderen

Rentenversicherungsträger folgen und bauen auf der geschilderten Basis in vielen Rechenzentren ihre elektronischen Archive auf.

Aktuell archiviert die Deutsche Rentenversicherung Bund Versicherungsunterlagen (Solokonten), Mikrofilmreproduktionen, Einheitsakten und Rehabilitationsbestandsakten. Ständig werden neue Unterlagen hinzugefügt, wie etwa der tägliche Posteingang per Hochleistungsscanner mit automatischer Barcode- oder OCR-Erkennung (Schriftenerkennung) für die Indizierung. Um später die Vorteile einer automatisierten Vorgangsbearbeitung richtig nutzen zu können, werden mit der digitalen Akte wichtige Vorarbeiten geleistet.

ZUSAMMENFASSUNG

- In Kapitel 9 haben wir die wichtigsten Anlässe zur Verarbeitung der Versicherungskonten kennen gelernt. Wir haben gesehen, dass Geschäftsprozesse die einzelnen Verarbeitungen beschreiben und wie diese Geschäftsprozesse unter Zuhilfenahme von Softwaretools
  modelliert werden. Durch den Einsatz von elektronischen Workflowsystemen in Verbindung mit der digitalen Aktenführung geht die Steuerung der Prozesse dabei verstärkt von der Sachbearbeitung auf die Maschine über.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

40. Welche Auslöser für eine Verarbeitung der Versicherungskonten kennen Sie?

41. Welche Arbeitsergebnisse erzeugen maschinelle Verarbeitungen in der Regel?

42. Was versteht man unter einem Geschäftsprozess?

43. Wie werden Geschäftsprozesse in der Regel dargestellt?

44. Wie unterscheiden sich bisherige IT-Unterstützung und Workflows?

45. Was geht sinnvollerweise mit der Einführung maschineller Vorgangsbearbeitungssysteme einher?

46. Welche Vorteile einer digitalen Akte können Sie nennen?

47. Welches sind die vier Hauptfunktionen der elektronischen Archivierung?

10. Online-Services

LERNZIELE

- Sie können die wichtigsten Online-Verfahren unter Nutzung der in den Versicherungskonten gespeicherten Daten benennen.
- Sie kennen die wichtigsten Online-Services und das Verfahren eSolution der Deutschen Rentenversicherung
- Sie können die datenschutzrechtlichen Voraussetzungen für die Online-Nutzung erklären.

Die Rentenversicherungsträger bieten ihren Kunden im Internet unter **www.deutsche-rentenversicherung.de** beziehungsweise in ihren jeweiligen Internetauftritten neben allgemeinen Informationen auch weitergehende Dienste an, wie zum Beispiel die Möglichkeit der elektronischen Antragstellung.
Dazu werden über ein spezielles Internetportal auch anderen Behörden und Datenlieferanten Auskunfts- und Datendienste (zum Beispiel zur Datenlieferung) zur Verfügung gestellt, um die Zusammenarbeit schneller und kostengünstiger zu gestalten. Eines dieser Verfahren ist eSolution.

Zur Wahrung des Sozialgeheimnisses haben die Träger der gesetzlichen Rentenversicherung in einer gemeinsamen Sicherheitsrichtlinie (Security Policy) festgelegt, unter welchen Voraussetzungen Versicherten der Online-Zugriff zu persönlichen Daten ermöglicht werden kann (§ 9 BDSG, Artikel 32 DSGVO).
Auch die Zulassung anderer Behörden zu den Online-Services folgt den gesetzlichen Regelungen im SGB X.

Mit dem Angebot solcher Online-Services, mit Zugriff auf die Bestände der Rentenversicherung, steigen auch die Anforderungen an die Verfügbarkeit der Anwendungen. Zur einer effektiven Online-Auskunft und -Beratung müssen die Datenverarbeitungssysteme der Rentenversicherungsträger und der DSRV daher zukünftig hochverfügbar (24/7) und für die Versicherten und Rentner zugänglich sein. Dieser 24-Stunden-Betrieb ist jedoch bei den meisten Versicherungsträgern noch nicht möglich. Dazu sind umfangreiche Änderungen der Systemkonzepte in den Datenverarbeitungssystemen und organisatorische Anpassungen erforderlich. Die RV-Träger haben sich im Jahr 2020 auf zeitgleiche Wartungsfenster geeinigt. Darüber hinaus werden sich im Rahmen der Rechenzentrumskonsolidierung weitere Verbesserungen der Servicezeiten ergeben.

10.1 rveServices der Deutschen Rentenversicherung

Mit der E-Government-Initiative „Bund Online 2005“ hat sich die Bundesregierung verpflichtet, bis zum Jahr 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung online anzubieten. Die Rentenversicherungsträger haben sich an dieser Initiative beteiligt.

Die Vorteile für die Kunden (Nutzende, Unternehmen, Verwaltungen), wenn Dienstleistungen über einen alternativen Zugangskanal online abgewickelt werden können, sind ein schneller, einfacher und unbürokratischer Abruf von Dienstleistungsangeboten, verbunden mit einer Erhöhung der Transparenz in der Dienstleistungserbringung durch eine stärkere Einbindung der Nutzenden in das Verwaltungshandeln. Um die elektronische Kommunikation mit der Verwaltung zu erleichtern, ist im August 2013 das Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) in Kraft getreten. Es ermöglicht Bund, Ländern und Kommunen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten.

Das E-Government-Gesetz verpflichtet die Verwaltung unter anderem dazu, einen elektronischen Zugang zu Verwaltungsleistungen zu eröffnen. Auch das Einreichen elektronischer Nachweise und die elektronische Bezahlung in Verwaltungsverfahren werden erleichtert. Darüber hinaus wurden Grundsätze der elektronischen Aktenführung und des ersetzenden Scannens festgelegt.

Mit dem Gesetz werden neben der qualifizierten elektronischen Signatur weitere sichere Technologien zugelassen, die die Schriftform gemäß § 36 a SGB I elektronisch ersetzen. Hierfür wurden zwei Technologien identifiziert, mit denen alle Funktionen der Schriftform abgebildet werden können:

- De-Mail mit der Versandoption "absenderbestätigt", welche eine sichere Anmeldung voraussetzt (Verfahren wird Mitte 2025 eingestellt).
- Web-Anwendungen der Verwaltung in Verbindung mit sicherer elektronischer Identifizierung durch die eID-Funktion des Personalausweises/ Aufenthaltstitel oder der Unionsbürgerkarte.

Mit E-Government verbindet sich für die Verwaltungen die Chance zum Einstieg in eine Internet-gestützte Dienstleistungskultur. Mit der Online-Bereitstellung von Dienstleistungen werden Möglichkeiten eröffnet, den Automationsgrad im Sinne einer durchgängigen elektronischen Vorgangsbearbeitung (Workflow) zu erhöhen. Auf der anderen Seite werden Synergieeffekte und Rationalisierungspotentiale für eine wirtschaftlichere Verwaltungsarbeit erschlossen.

Ein weiterer Schritt zur flächendeckenden Digitalisierung der Verwaltung Deutschlands ist das im August 2017 in Kraft getretene Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG). Danach sollten bis 2023 der Bund, Länder und die Kommunen alle Verwaltungsleistungen in Deutschland über Verwaltungsportale auch digital anbieten und diese Portale zu einem Verbund verknüpfen. Das OZG sieht somit die Vernetzung von Bund, Ländern und Kommunen als Gemeinschaftsaufgabe an.

Mit der Einführung des OZG-Änderungsgesetzes (OZG 2.0) im Februar 2024 wird die Digitalisierung der Verwaltung als Daueraufgabe beschlossen. Die wichtigsten Maßnahmen sind die

- Fokussierung auf die Ende-zu-Ende-Digitalisierung
- Festlegung eines einheitlichen Bürger- und Organisationskontos,
- Once-Only-Generalklausel, mit der der Abruf benötigter Nachweise bei anderen Behörden ermöglicht wird,
- faktische Abschaffung der Schriftform
- Bereitstellung von relevanten Standards und Schnittstellen durch das Bundesministeriums des Innern und für Heimat (BMI).

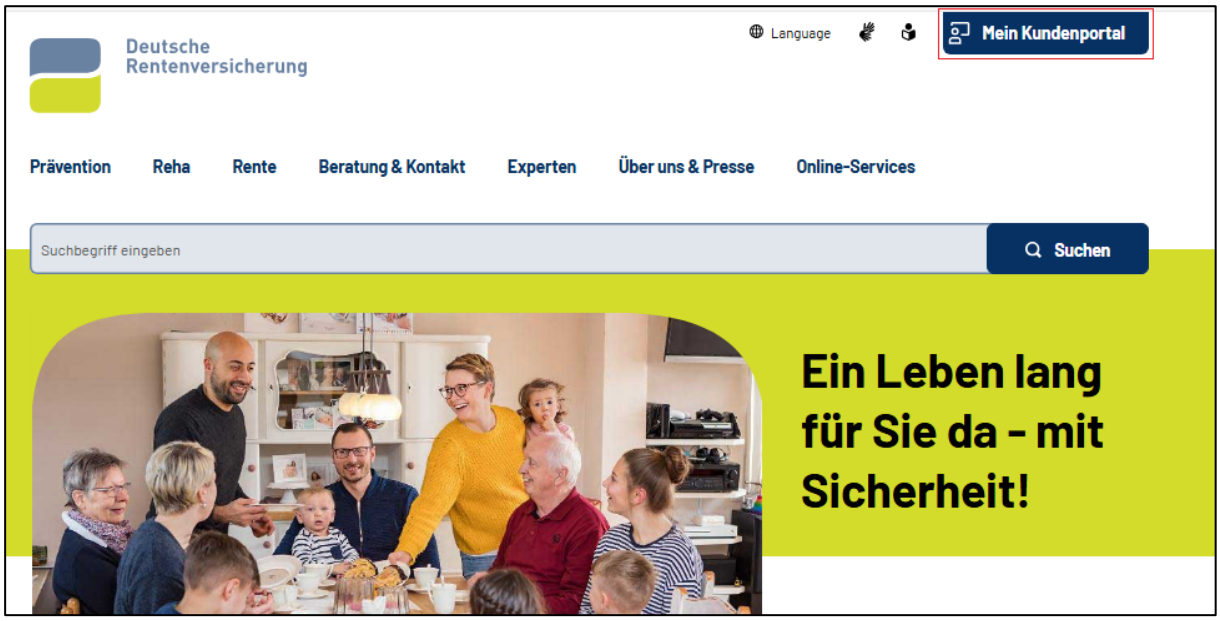
10.2 Informationsdienste, Broschüren

Die erste Stufe elektronischer Dienstleistungen stellen die Informationsangebote der Rentenversicherungsträger dar, die sich entweder an bestimmte Personengruppen richten (wie zum Beispiel Arbeitgeber, Berufsanfänger, Versicherte und Rentner*innen) oder sich an bestimmten Lebenslagen orientieren (zum Beispiel Beschäftigungsaufnahme, Kindererziehung, Prävention, Rehabilitation, Arbeiten im Ausland). Hierzu gehört auch die Bestellung von Broschüren sowie Antragsvordrucken und deren direkter Download über das Internet.

10.3 Das Kundenportal der Deutschen Rentenversicherung

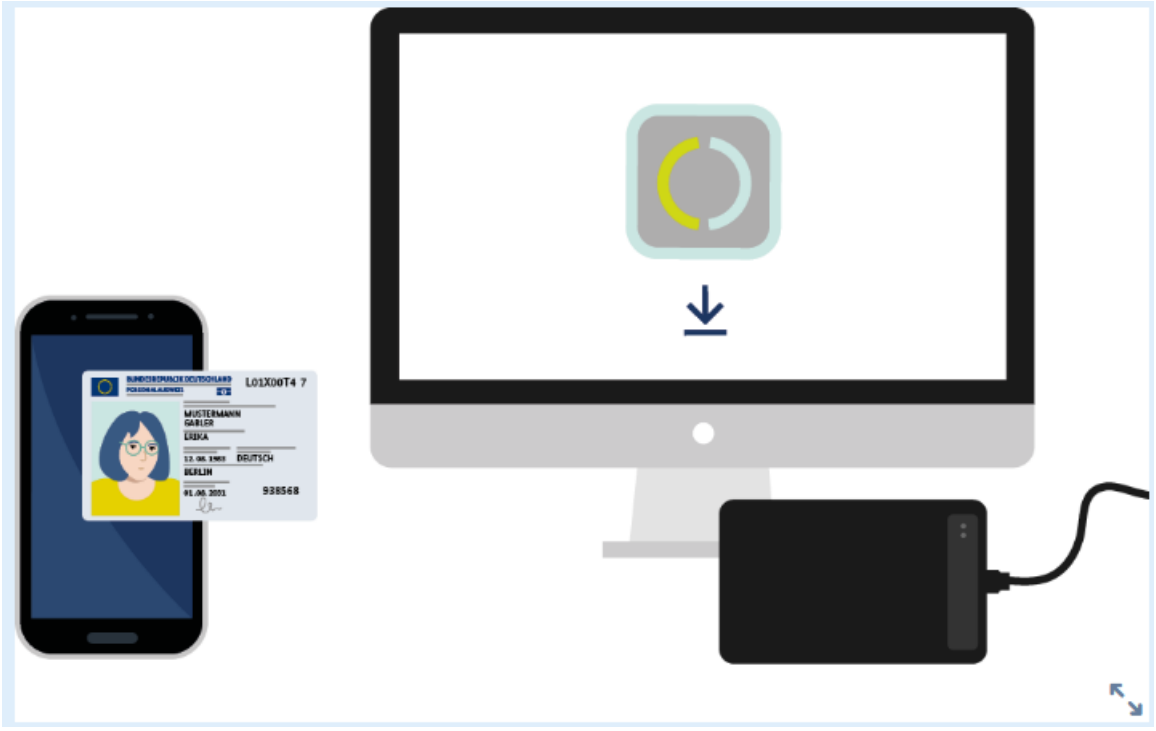
Das Kundenportal ist von allen Internetseiten der DRV einheitlich erreichbar.

Abbildung 14: Einstieg Kundenportal



Für das Kundenportal wird ein Personalausweis, ein elektronischer Aufenthaltstitel oder eine Unionsbürgerkarte mit elektronischem Identitätsnachweis (eID) beziehungsweise eine Signaturkarte benötigt. Beim jeweiligen Ausweisdokument muss die Online-Ausweisfunktion (eID) freigeschaltet sein. Das geschieht automatisch bei der Ausweisausgabe.
Darüber hinaus ist der Zugang auch mithilfe der nationalen elektronischen Identität als EU-Bürger oder Bürgerin nach der eIDAS möglich.

Abbildung 15: ID Check zum Nutzen digitaler Angebote



ID Check mit der AusweisApp

Um sich online erfolgreich zu identifizieren, werden drei Dinge benötigt:

1. die aktivierte Online-Ausweisfunktion,

2. das physisches Ausweisdokument und

3. die AusweisApp.

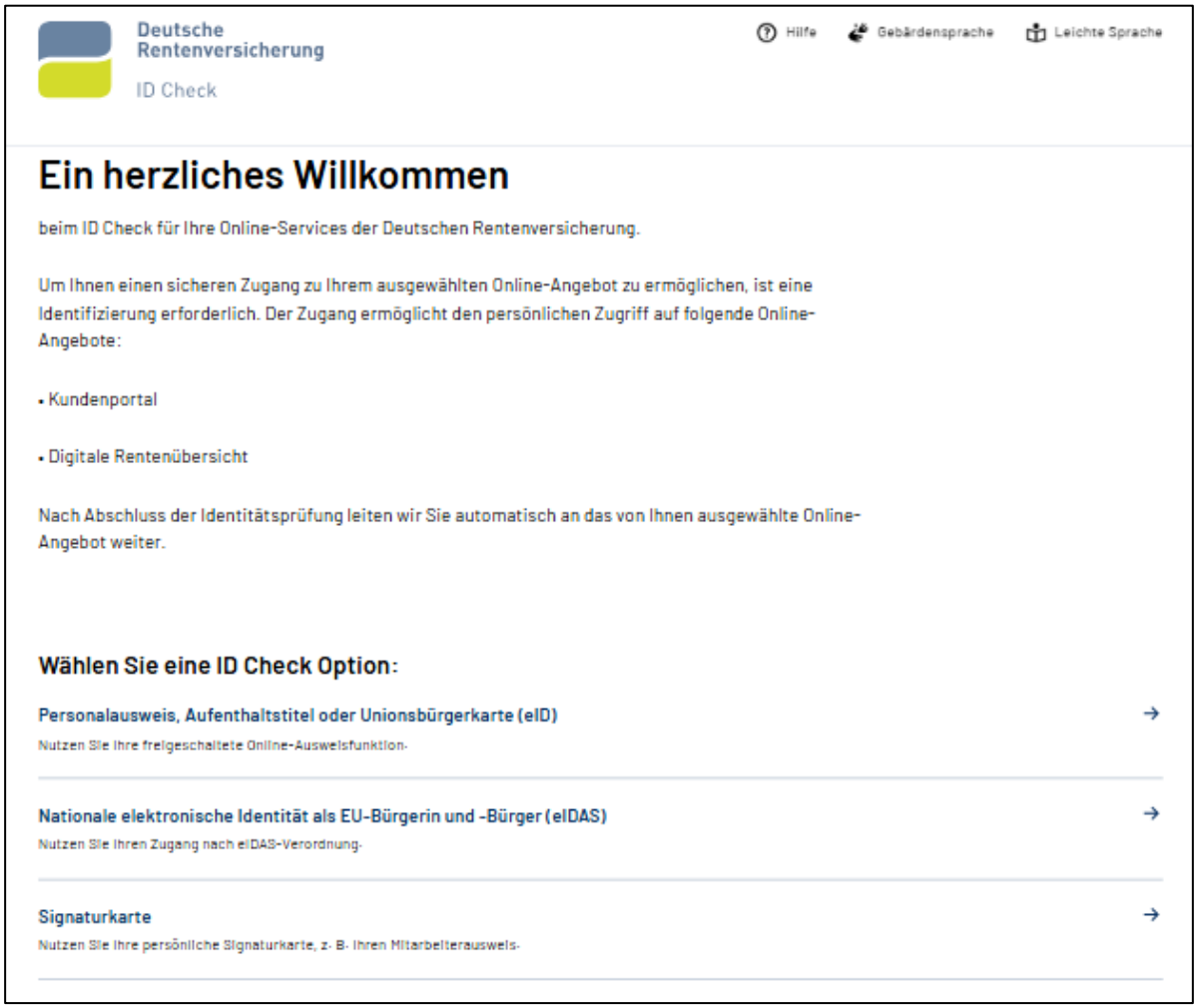
Die AusweisApp kann über ein Smartphone oder Tablet kostenlos im Google Play Store oder im Apple App Store herunterladen werden.
Um die AusweisApp nutzen zu können, wird jedoch ein NFC-fähiges Smartphone oder Tablet benötigt.

ID Check mit Kartenlesegerät

Alternativ kann der ID Check mit dem Ausweisdokument und einem USB-Kartenlesegerät durchführt werden. Dazu muss die AusweisApp auf dem Computer installiert sein.

Der ID Check ermöglicht einen sicheren Zugang zum Leistungsspektrums des Kundenportals. Die zentrale Authentifizierungs- und Registrierungskomponente gem. § 138 Absatz 1 Satz 2 Nummer 10 SGB VI wird bei der bei der DSRV in Würzburg betrieben (siehe Kapitel 4.2).

Abbildung 16: ID Check der Deutschen Rentenversicherung

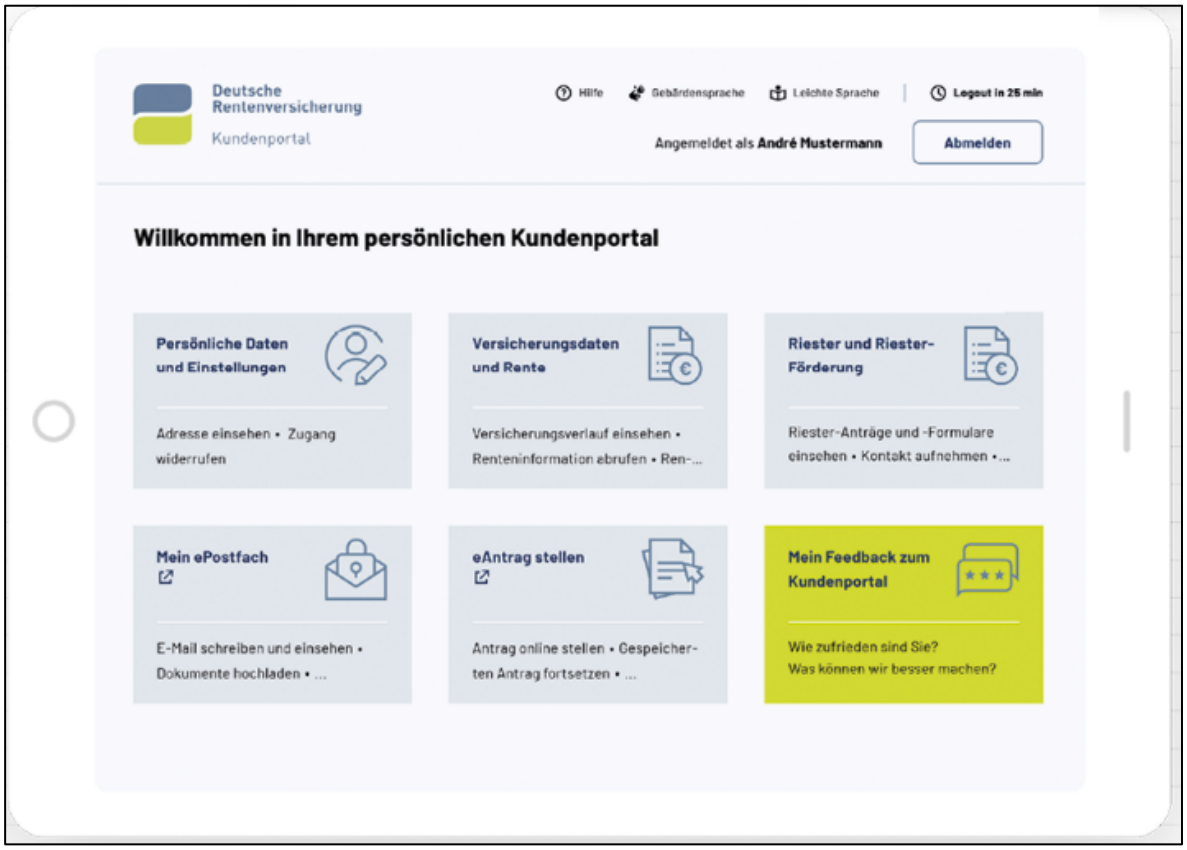


Nach dem Durchlaufen des Registrierungs- oder Anmeldeprozesses öffnet sich der geschützte Bereich des Kundenportals, in welchem Anliegen rund um die Themen Rente, Rehabilitation, Versicherung und Riester-Rente erledigt werden können.

Im persönlichen Kundenportal befinden sich Online-Services zentral an einem Ort – von A wie „Antrag stellen“ bis Z wie „Zugang widerrufen“, zum Beispiel:

- sicherer Zugang: optimaler Schutz der persönlichen Daten
- Zugriff und Änderung von persönlichen Daten: einfach, schnell und sicher
- Anträge zu Rente, Rehabilitation oder Riester stellen und verwalten Versicherungsverlauf, Renteninformation und Rentenauskunft jederzeit abrufbar

Abbildung 17: Das Kundenportal der Deutschen Rentenversicherung



Im Bereich der Persönlichen Daten und Einstellungen haben Nutzende die für die Deutsche Rentenversicherung relevanten persönlichen Daten hinterlegt. Beispielsweise kann hier die Versicherungsnummer als auch der zuständige Rentenversicherungsträger eingesehen werden. Darüber hinaus besteht die Möglichkeit, die gespeicherte Anschrift zu ändern. Die geänderten persönlichen Daten stehen sofort elektronisch zur Verfügung und bilden so den Einstieg in vollautomatisierte Workflowsysteme (siehe auch Kapitel 9).

Über die Versicherungsdaten und Rente haben Nutzende einen Zugang zu persönlichen Auskünften zu den Themen Versicherung und Rente. Beispielsweise kann hier die Rentenauskunft angefordert werden. Diese wird dann als PDF zum Download oder aber zur Einsichtnahme zur Verfügung gestellt.

Über die Kachel Riester und Riester-Förderung besteht die Möglichkeit, Riesteranträge zu stellen, Informationen rund um die Riesterförderung zu erhalten und mit der Zentralen Stelle für Altersvermögen in persönlichen Kontakt zu treten.

Sofern Nutzende beabsichtigen, eine elektronische Nachricht an die Deutsche Rentenversicherung zu senden, ist dies mit dem elektronischen Postfach sicher möglich. Das ePostfach ist der digitale Briefkasten für persönliche Nachrichten. Hier können auch Dokumente und Bescheinigungen ganz einfach digital übermittelt und anschließend in individuelle Ordner sortiert werden.
Damit der Rentenversicherungsträger vollelektronisch antworten kann, benötigt die Deutsche Rentenversicherung die Zustimmung des Nutzenden. Hierfür kann der Online-Service Elektronische Kommunikation verwalten verwendet werden.

Im Bereich eAntrag stellen haben die Nutzenden einen unkomplizierten direkten Draht zum Rentenversicherungsträger. Durch die Registrierung und Anmeldung im Kundenportal erfragt das Antragsverfahren bereits während der Antragstellung die im Versicherungskonto

gespeicherten Daten. So können die Angaben im Antrag vor und bei Eingabe auf Plausibilität geprüft werden. Zeitaufwändige Rückfragen werden dadurch minimiert.

10.3.1 Die Online-Services ohne Identifikation

Mit den Online-Services der Deutschen Rentenversicherung können derzeit verschiedene Online-Leistungen ohne Identifikation durch unseren Nutzenden beansprucht werden. Bei der nachfolgenden Aufzählung handelt es sich um Beispiele:

- Anforderung von Druckprodukten: Versicherungsverlauf, Rentenauskunft, Rentenbezugsbescheinigung für das Finanzamt
- Stellen von Anträgen
- Vereinbaren von Terminen
- Nutzung von Online-Rechner.

Abbildung 18: Online-Service ohne Identifikation

10.3.2 Online-Service: Antrag stellen

Mit der Webversion Antrag stellen können Versicherte, Rentner*innen und Hinterbliebene elektronische Anträge in den Themenbereichen Versicherung, Rehabilitation und Rente online stellen. Die Anträge stehen auch berechtigten Dritten, zum Beispiel Betreuenden und Bevollmächtigten, zur Verfügung.

Bei Antrag stellen (eAntrag) handelt es sich um die Weiterentwicklung von Antrag Online. Den Antragstellenden steht eine Online-Hilfe zur Verfügung, die sie bei unklaren Fragestellungen unterstützt und auf Eingabefehler hinweist. Auf Wunsch können Antragstellende einen Bescheid elektronisch in das ePostfach der DRV erhalten. Hierfür ist im Kundenportal die Zustimmung zur elektronischen Kommunikation zu erteilen.

Auch für die Gemeinde- und Versicherungsämter, Versichertenälteste und Versichertenberater sowie für die Auskunft- und Beratungsstellen - die bislang die PC-Anwendung „Antrag-Online“ nutzen – wurde der Umgang im Rahmen der Antragsaufnahme durch die Expertenversion von eAntrag einfacher, komfortabler, kostengünstiger und unkomplizierter. Mit dieser Anwendung können autorisierte Nutzende Anträge für Versicherte/Rentner*innen und Hinterbliebene online ausfüllen und elektronisch weiterleiten.

Je nach Authentifizierungsmethode werden die bereits im Versicherungskonto bekannten Daten ergänzt beziehungsweise die Fragen nicht mehr gestellt. Nur fehlende Informationen werden abgefragt. eAntrag kann auch mit verschachtelten Anträgen (Antrag in einem Antrag) umgehen. Je nach Eingabe blendet die intelligente Formularführung unwichtige Bereiche aus und gestaltet die Eingabe somit übersichtlicher.

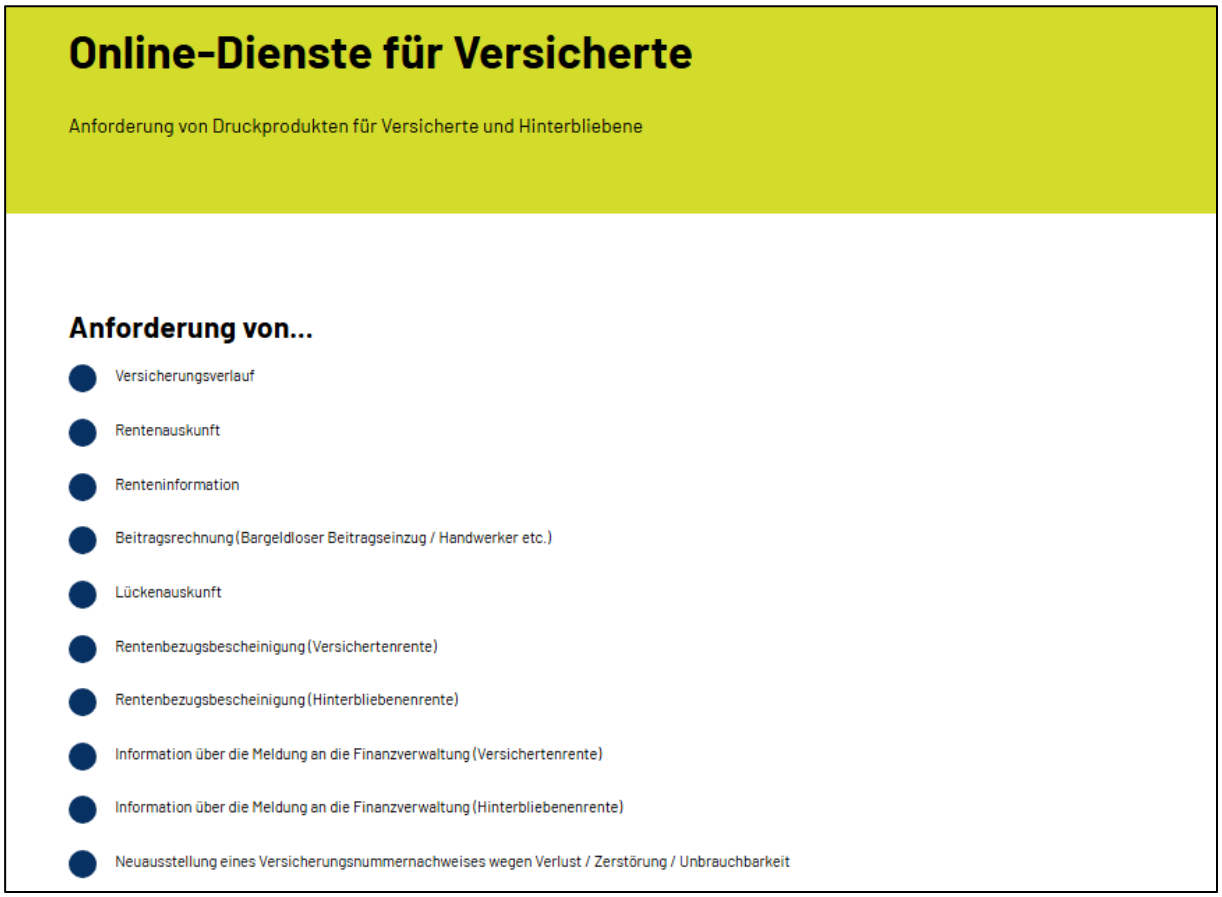
Die erfassten Antragsdaten stehen sofort elektronisch zur Verfügung und bilden so den Einstieg in vollautomatisierte Workflowsysteme (siehe auch Kapitel 9). Die Möglichkeiten dieser Automatisierung sind ein wichtiger Input für die weitere Entwicklung von rvSystem.

10.3.3 Online-Service: Versicherungsunterlagen anfordern

Die Online-Service ohne Identifikation dient der Beantragung von personifizierten Informationen in Form von Druckprodukten. Allerdings erfolgt die Zusendung der Schriftstücke auf dem Postweg an die im Versicherungskonto gespeicherte Adresse. Eine Anzeige der Druckprodukte kann in diesem Fall online nicht erfolgen, da eine vorherige Registrierung oder Anmeldung fehlt und der Nutzende beziehungsweise Anfordernde damit nicht bekannt ist.

Mit dem Online-Service Versicherungsunterlagen anfordern können Versicherte zurzeit folgende Informationen abrufen:

Abbildung 19: Anforderung von Druckprodukten



Der Online-Service wird ab 2025 modernisiert.

10.3.4 Online-Service: Persönliche Daten ändern

Über persönliche Daten ändern können Nutzende ihre Anschrift oder Bankverbindung ändern.

Hat sich die Anschrift geändert, können Versicherte mithilfe eines elektronischen Formulars über Antrag stellen die Änderungsmitteilung an den Rentenversicherungsträger weitergeben.

Rentenempfänger hingeben werden an den Renten Service zur Bekanntgabe der neuen Anschrift weitergeleitet.

Ähnlich verhält es sich bei der Bankverbindung. Handelt es sich beim Anfragenden um einen Rentner, erfolgt das Weiterleiten an den Renten Service.

Im Bereich der freiwilligen Beitragszahlung, beim Abbuchen von Pflichtbeiträgen oder bei Rehabilitationssachverhalten gibt es die Möglichkeit, das elektronische Kontaktformular für persönliche Anliegen über die elektronische Antragstellung zu nutzen.

10.3.5 Online-Service: Termine vereinbaren

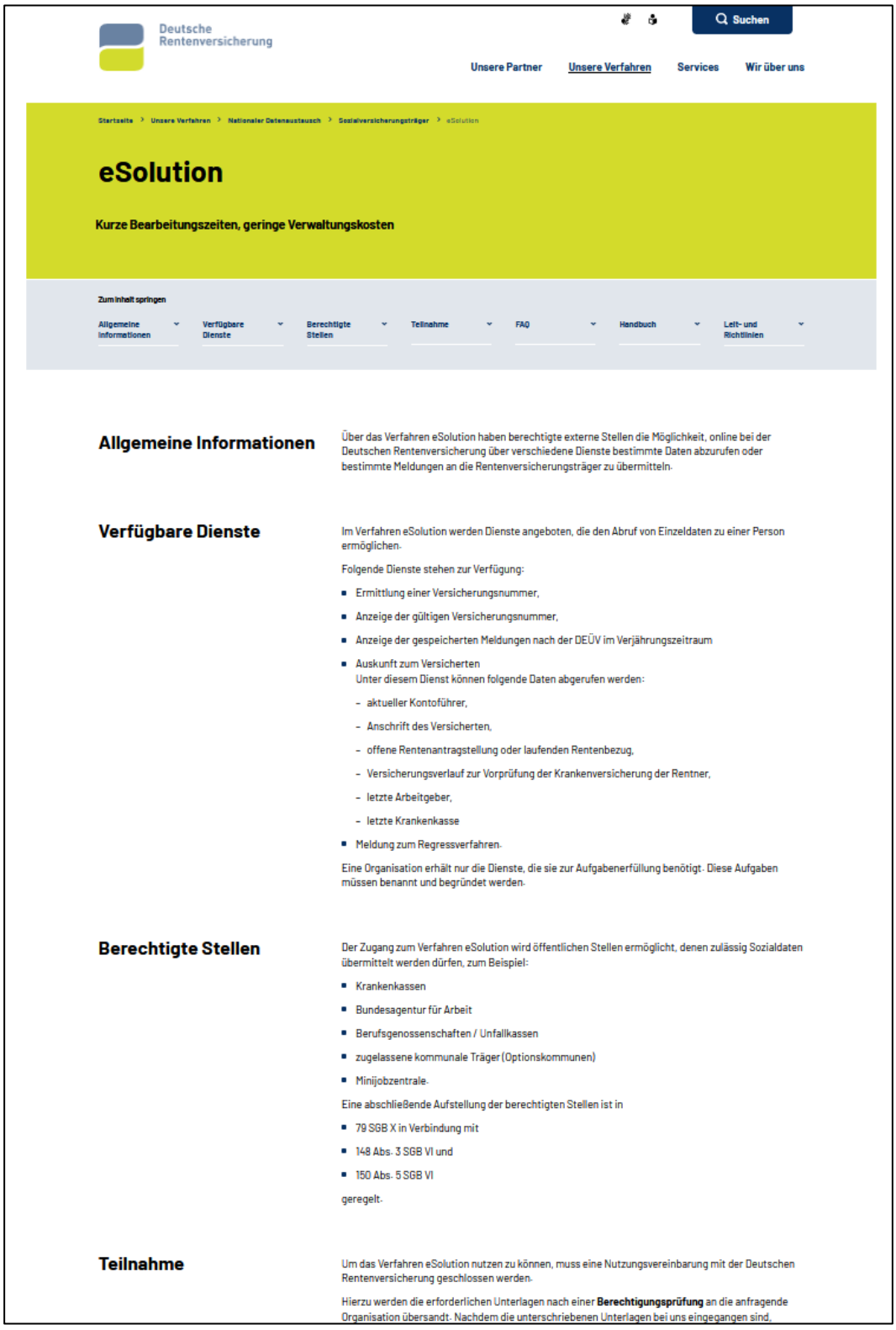
Mit diesem Online-Service haben Versicherte/ Rentner die Möglichkeit, einen festen Beratungstermin online zu buchen. Eine Authentifizierung ist nicht erforderlich.
Über den Service können die Nutzenden eine gewünschte Beratungsstelle, das Anliegen und den Wunschtermin auswählen. Je nach Verfügbarkeit freier Termine und der voraussichtlichen Beratungsdauer wird ein Vorschlag für einen verbindlichen Beratungstermin erstellt, der durch die Nutzenden bestätigt werden muss.

Dieser Online-Service wurde modernisiert und steht auf unserer Webseite zur Verfügung.

10.4 Verfahren "eSolution" der Deutschen Rentenversicherung

Das Verfahren „eSolution“ der Deutschen Rentenversicherung richtet sich, anders als die Online-Services, nicht an die Versicherten, sondern zielt auf verschiedene Organisationen (z.B. Krankenkassen, Bundesagentur für Arbeit, Jobcenter, Berufsgenossenschaften) ab.

Abbildung 20: Informationsseite zum Verfahren eSolution auf der Seite der DSRV (www.dsrv.info/esolution)



Deutsche Rentenversicherung

Suchen

Unsere Partner | Unsere Verfahren | Services | Wir über uns

Startseite > Unsere Verfahren > Nationaler Datenaustausch > Sozialversicherungsträger > eSolution

eSolution

Kurze Bearbeitungszeiten, geringe Verwaltungskosten

Zum Inhalt springen

Allgemeine Informationen | Verfügbare Dienste | Berechtigte Stellen | Teilnahme | FAQ | Handbuch | Leit- und Richtlinien

Allgemeine Informationen

Über das Verfahren eSolution haben berechtigte externe Stellen die Möglichkeit, online bei der Deutschen Rentenversicherung über verschiedene Dienste bestimmte Daten abzurufen oder bestimmte Meldungen an die Rentenversicherungsträger zu übermitteln.

Verfügbare Dienste

Im Verfahren eSolution werden Dienste angeboten, die den Abruf von Einzeldaten zu einer Person ermöglichen.

Folgende Dienste stehen zur Verfügung:

- Ermittlung einer Versicherungsnummer,
- Anzeige der gültigen Versicherungsnummer,
- Anzeige der gespeicherten Meldungen nach der DEÜV im Verjährungszeitraum
- Auskunft zum Versicherten
  Unter diesem Dienst können folgende Daten abgerufen werden:
  - aktueller Kontoführer,
  - Anschrift des Versicherten,
  - offene Rentenantragstellung oder laufenden Rentenbezug,
  - Versicherungsverlauf zur Vorprüfung der Krankenversicherung der Rentner,
  - letzte Arbeitgeber,
  - letzte Krankenkasse
- Meldung zum Regressverfahren.

Eine Organisation erhält nur die Dienste, die sie zur Aufgabenerfüllung benötigt. Diese Aufgaben müssen benannt und begründet werden.

Berechtigte Stellen

Der Zugang zum Verfahren eSolution wird öffentlichen Stellen ermöglicht, denen zulässig Sozialdaten übermittelt werden dürfen, zum Beispiel:

- Krankenkassen
- Bundesagentur für Arbeit
- Berufsgenossenschaften / Unfallkassen
- zugelassene kommunale Träger (Optionskommunen)
- Minijobzentrale.

Eine abschließende Aufstellung der berechtigten Stellen ist in

- 79 SGB X in Verbindung mit
- 148 Abs. 3 SGB VI und
- 150 Abs. 5 SGB VI

geregelt.

Teilnahme

Um das Verfahren eSolution nutzen zu können, muss eine Nutzungsvereinbarung mit der Deutschen Rentenversicherung geschlossen werden.

Hierzu werden die erforderlichen Unterlagen nach einer **Berechtigungsprüfung** an die anfragende Organisation übersandt. Nachdem die unterschriebenen Unterlagen bei uns eingegangen sind,

Das Verfahren eSolution ist eine Webanwendung, welche mit verschiedenen Diensten Einzelabfragen externer Kunden ermöglicht.

Die zur Verfügung stehenden Dienste sind:

- Ermittlung der Versicherungsnummer,
- Anzeige der gültigen Versicherungsnummer
- Anzeige der gespeicherten Meldungen nach der DEÜV im Verjährungszeitraum

und

- Auskunft zum Versicherten

Unter diesem Menüeintrag kann der Nutzer folgende Daten zum Versicherten abrufen

- Kontoführer,
- Anschrift,
- Rentenantragstellung oder eines laufenden Rentenbezuges, sofern vorhanden,
- Anschrift der letzten bekannten Krankenkasse,
- Anschrift des letzten bekannten Arbeitgebers

und

- Versicherungsverlauf zur Vorprüfung der KVdR
- Meldung zum Regressverfahren

Seit Ende Januar 2024 gibt es einen neuen Dienst der die Übermittlung der Regressmeldung nach § 119 SGB X von den Krankenkassen/Berufsgenossenschaften/Bundesagentur für Arbeit an den jeweils zuständigen Rentenversicherungsträger ermöglicht. Dieser Dienst ist der erste im Verfahren eSolution der es ermöglicht Daten von dritten Stellen über eSolution an rvSystem zu übermitteln.

Die zwischen den externen Datenstellen und den Trägern der Rentenversicherung vorhandenen automatisierten Massenverarbeitungsverfahren (Batch-Verfahren, Meldeverfahren) sind hiervon nicht betroffen.

Die dabei angestrebten Ziele liegen im strategischen Bereich oder sie beabsichtigen die Verbesserung der Geschäftsprozesse und der IT-Unterstützung:

- Verbesserte Unternehmenskommunikation,
- Schaffung eines zentralen Unternehmenszugangs für Kunden,
- Steigerung der Kundenzufriedenheit,
- Kostensenkung (Verwaltungs- und Verfahrenskosten) durch Vermeidung von Medienbrüchen und Verringerung von Laufzeiten,
- Erhöhung der Prozess- und Servicequalität durch Reduktion und Harmonisierung,
- Automatisierung von Prozessen und Nutzung von Standards,
- IT- und Datenkonsolidierung, Integration von Anwendungssystemen.

10.5 Stammsatz-Auskunft-Online

Die Deutsche Rentenversicherung hat mit der Stammsatzauskunft eines der wesentlichen Auskunftsverfahren online zur Verfügung gestellt. Dabei wurde der Schwerpunkt auf individuelle, kundenspezifische Auskunftsfunktionen gelegt, die durch die sichere Authentifizierung des Anfragenden mittels Benutzerkennung und Passwort abgesichert wurden.

Alle Auskunftsverfahren erfolgen dabei im Dialog. Es wird zwischen zwei Stammsatzauskunftsarten unterschieden:

- Anfrage mit Versicherungsnummer

- Anfrage mit persönlichen Daten wie Geburtsdatum, Namen, Anschrift (Alpha-Suche), sofern die Versicherungsnummer nicht bekannt ist. Eine Suche über Wortteile mit Wildcards (? oder *) ist möglich.

Die Berechtigung, die Anwendung Stammsatzauskunft ausführen zu dürfen, wird über Transaktions- und Programmschutz geregelt. Die Zugriffsberechtigungen werden über Benutzerkennung gewährleistet und zentral verwaltet.

Der Web-Dienst wertet den empfangenen Datensatz aus und stellt dem Anfrager das Ergebnis (Versicherungsnummer und persönliche Daten) als Bildschirmansicht dar, sofern eindeutige Treffer erzielt werden konnten. Das Ergebnis kann auch druckaufbereitet werden.

10.6 Elektronischer Rechtsverkehr

Im elektronischen Rechtsverkehr geht es darum, Schriftstücke und Dokumente elektronisch dem Empfänger zukommen zu lassen. Dokumente, die eine Rechtswirkung entfalten, waren häufig an das Schriftformerfordernis und das Erfordernis der eigenhändigen Unterschrift gebunden. (zum Beispiel Einreichung Klage, Widerspruch, etc.)

Der Gesetzgeber hat inzwischen Regelungen über elektronische Dokumente getroffen und Übermittlungswege geschaffen, die eine sichere, rechtsverbindliche Kommunikation auf elektronischem Weg ermöglichen. Seit dem 1. Januar 2022 ist die Nutzung des ERV für Rechtsanwälte, Behörden sowie juristische Personen des öffentlichen Rechts verpflichtend (§ 130d ZPO).

Elektronisches Gerichts- und Verwaltungspostfach (EGVP)

EGVP bezeichnet als Oberbegriff das elektronische Gerichts- und Verwaltungspostfach und die damit verbundene technische Infrastruktur. Damit ein EGVP eine besondere „Rolle“ erhält, z.B. als beBPo (besonderes elektronisches Behördenpostfach) oder beA (besonderes elektronisches Anwaltpostfach), muss sich der Inhaber des Postfachs vor seiner Aufsichts-/Prüfbehörde identifizieren. Nach dieser Identifizierung wird das Postfach im jeweiligen Verzeichnisdienst freigeschaltet. Dabei erhält jedes Postfach eine sog. „SAFE ID“ als Identifizierungs- und Adressierungskennzeichen. Nachrichten aus einem identifizierten Postfach fallen unter den Begriff des „sicheren Übermittlungsweges“.

Die technische Infrastruktur beruht auf dem Kommunikations-Standard OSCI (Online Services Computer Interface). OSCI ist der Name eines Protokollstandards für die deutsche öffentliche Verwaltung. OSCI-Transport steht für die sichere, vertrauliche und rechtsverbindliche Übertragung digitaler Daten über das Internet.

Die DSRV betreibt seit Juli 2020 für jeden Rentenversicherungsträger ein beBPo, über das Nachrichten im elektronischen Rechtsverkehr ein- und ausgehen. An die beBPo‘s sind Fachanwendungen, wie z.B. die Verfahren eGericht, eVA oder eGerichtsvollzieher angebunden. Wenn die Nachricht vorgeschriebene oder vereinbarte Standards erfüllt, kann der Inhalt der Nachricht in die jeweiligen Fachverfahren, z.B. in das Verfahren eGericht weitergeleitet werden.

XJustiz Standard

XJustiz ist ein bundeseinheitlicher Standard für das Datenaustauschformat im elektronischen Rechtsverkehr. Unter Verwendung von XML-Schema-Dateien werden strukturierte Daten im xml-Format übergeben. Der Standard legt die zu nutzenden Datenstrukturen für die

jeweiligen Nachrichtentypen und Schlüsseltabellen fest, z.B. wird definiert an welcher Stelle der XML Datei die Adresse des Beteiligten zu stehen hat oder dass der Code "000" für "Deutschland" steht. Der Standard wird in der XJustiz Spezifikation festgeschrieben und jährlich überarbeitet.
Die XJustiz-Nachricht wird der EGVP-Nachricht als Anhang (Attachment) beigefügt.

10.7 Datenaustausch im elektronischen Rechtsverkehr

10.7.1 eGericht

Die Deutsche Rentenversicherung bietet die Möglichkeit zur rechtssicheren, elektronischen Kommunikation im Rahmen des elektronischen Rechtsverkehrs (ERV). Dies betrifft insbesondere den Austausch mit Gerichten, Rechtsanwältinnen und Rechtsanwälten, Behörden sowie sonstigen Verfahrensbeteiligten.

Zunächst wurde 2012 für den elektronischen Rechtsverkehr mit der Sozialgerichtsbarkeit ein sicheres elektronisches Verfahren entwickelt, mit dessen Hilfe Dokumente zwischen allen Rentenversicherungsträgern und allen Sozialgerichten in beiden Richtungen ausgetauscht werden können.
Ab dem 01.01.2018 mussten die Träger der Rentenversicherung in der Lage sein, von allen Gerichtszweigen elektronische Nachrichten über das EGVP/beBPo anzunehmen und zu beantworten. Die entsprechenden Regelungen hierzu enthielt das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013 (BGBl. Seite 3786).

Für die Umsetzung der gesetzlichen Vorgabe wurde das Verfahren eSozialgericht um die anderen Gerichtszweige ergänzt, um andere Funktionalitäten erweitert und zum Verfahren "eGericht" ausgebaut.

Die Gerichte senden per EGVP einen XJustiz Datensatz, in dem auf beiliegende Dokumente referenziert wird. Neben dem XJustiz Datensatz enthält die EGVP-Nachricht die referenzierten Dokumente. So können sämtliche PDF-Dateien sicher zwischen Gerichten und der Deutschen Rentenversicherung versandt werden.

Innerhalb der Deutschen Rentenversicherung erfolgt die Überwachung und Protokollierung der ein- und ausgehenden Nachrichten (Monitoring-Verfahren), die Speicherung in der Kommunikations-Datenbank sowie die Transformation zwischen XJustiz-Datensatz und den Einzelfeldern, die in jeweiligen Fach-Datenbanken gespeichert werden.

Die Fachanwendung „eGericht“ ist ein Dialogverfahren, das von den zuständigen Anwendern aller Rentenversicherungsträger genutzt werden kann. Es enthält Funktionalitäten zur

- Verwaltung von Nachrichten,
- zur Benutzerverwaltung und
- zur Datenpflege der teilnehmenden Gerichte.

Es zeigt ein- und ausgehende Nachrichten nach bestimmten Filterkriterien an und ermöglicht das Erstellen, die Adressierung und das Versenden neuer Nachrichten. Die Benutzerverwaltung beinhaltet die Eingabe und Änderung von Daten zu Struktureinheiten und Personen, die die Anwendung nutzen sollen, und ermöglicht die Authentifizierung der Benutzer beim Aufruf des Dialogverfahrens.

Geschäftsvorfälle werden dadurch vollmaschinell, effizient und sicher verarbeitet. Dadurch ist eine enorme Kostenersparnis bei der DRV und den Gerichten möglich.

Neben Kostenvorteilen durch interne Effizienzgewinne (Reduzierung von allgemeinen Anfragen und Versandaufwand, reduzierte Transaktionskosten) besteht auch Einsparpotenzial bei Druckkosten (Papier und Verbrauchsmaterialien) sowie Portokosten.

Des Weiteren werden alle Nachrichten der Sozialgerichte mit VSNR über einen Fachdienst direkt dem Archiv und damit der digitalen Leistungsakte des jeweiligen RV-Trägers zur Verfügung gestellt. Die Antwort an das Sozialgericht kann über das Textsystem der Rentenversicherung rvText ebenfalls elektronisch erfolgen. Damit wurde ein weiterer Schritt in Richtung durchgängiger elektronischer Workflow gelegt.

Durch das Gesetz zum elektronischen Rechtsverkehr und der dazugehörigen Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) sind die Träger der Rentenversicherung seit 01.01.2022 verpflichtet, alle Nachrichten, die im Rahmen des eröffneten elektronischen Rechtsweges zugestellt werden, auch rechtsverbindlich anzunehmen.

Daher ist das Verfahren eGericht inzwischen zur "zentralen Poststelle" des elektronischen Rechtsverkehrs geworden. Neben der Kommunikation mit Gerichten gehen in den beBPos der Rentenversicherungsträger auch Nachrichten von Rechtsanwälten, Notaren, Betreuern, Kliniken, Steuerberatern und sogar Privatpersonen ein.

Im Jahr 2024 wurden über 1.139.513 Nachrichten im elektronischen Rechtsverkehr empfangen und an die Träger weitergeleitet sowie über 311.566 Nachrichten versandt.

Elektronischer Versorgungsausgleich (eVA)

Seit 1977 findet bei einer Ehescheidung regelmäßig ein Versorgungsausgleich statt. Dabei werden die in der Ehe erworbenen Versorgungsanrechte gleichmäßig zwischen den Eheleuten aufgeteilt. Zur Vorbereitung des Versorgungsausgleichs holt das Familiengericht von den beteiligten Versorgungsträgern Auskünfte über die Höhe der von den Eheleuten jeweils erworbenen Versorgungsanrechte ein. Die Entscheidung über den Versorgungsausgleich trifft ebenfalls das Familiengericht, das zugleich über die Durchführung des Ausgleichs einen Beschluss erlässt. Dieser wird den Eheleuten sowie den beteiligten Versorgungsträgern in Form einer beglaubigten Abschrift übersandt. Zu gegebener Zeit informiert das Familiengericht die Eheleute sowie die beteiligten Versorgungsträger über den Eintritt der Rechtskraft.

Dieses Verfahren erfordert eine umfassende Kommunikation und einen umfangreichen Austausch von Daten zwischen den Familiengerichten und den Rentenversicherungsträgern. Ohne Besonderheiten sind in der Regel fünf Nachrichten pro Person auszutauschen. Zugleich handelt es sich um ein Massengeschäft, da im Durchschnitt der letzten 20 Jahre mehr als 162.000 Ehen pro Jahr geschieden wurden (Quelle https://de.statista.com/statistik/daten/studie/228/umfrage/anzahl-der-ehescheidungen-seit-1990) und daran über 324.200 Eheleute beteiligt sind. Hat jede dieser Personen während der Ehezeit Anrechte in der gesetzlichen Rentenversicherung erworben, sind von den Rentenversicherungsträgern 324.200 Auskünfte pro Jahr zu erteilen und von den Familiengerichten zu verarbeiten. Die Verfahrensabläufe hierzu sind geprägt durch Standardisierungen und Wiederholungen.

Das Verfahren zum Versorgungsausgleich eignete sich deshalb für einen elektronischen Datenaustausch. Die bisherige Kommunikation auf dem Postweg zwischen den Familiengerichten und der Deutschen Rentenversicherung wurde durch eine internetbasierte Lösung ersetzt.

Die gesetzliche Grundlage hierzu ist mit § 229 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) mit Wirkung zum 01.09.2009 geschaffen worden. Nach Absatz 3 Satz 1 des § 229 FamFG sind die Familiengerichte und die Versorgungsträger im Auskunftsverfahren nach § 220 FamFG verpflichtet, am elektronischen Übermittlungsverfahren teilzunehmen, sofern die technischen Voraussetzungen hierfür geschaffen worden sind.

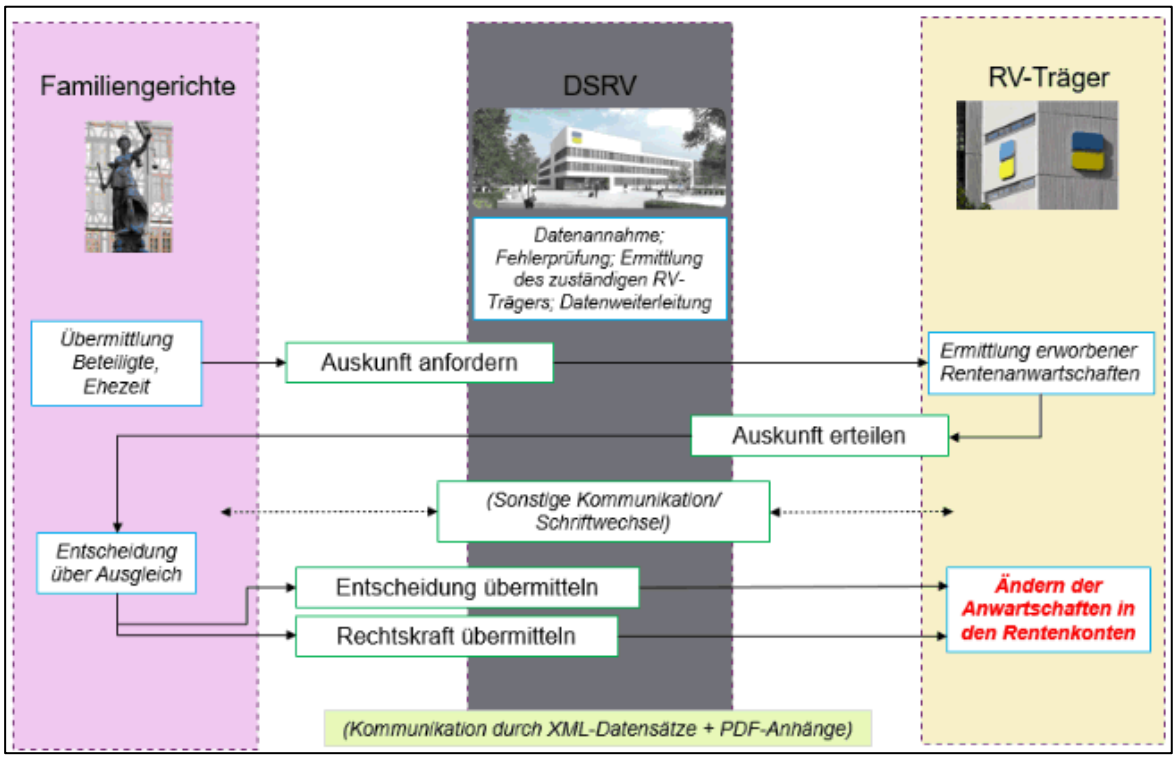
Zur Übermittlung von Nachrichten zwischen den Familiengerichten und der Deutschen Rentenversicherung wird die EGVP-Infrastruktur genutzt.

Nachrichtentypen, deren Struktur und Inhalt sind im XJustiz Standard, Fachmodul Versorgungsausgleich, definiert.

Wenn beim Gericht die Versicherungsnummer nicht bekannt ist, wird diese zunächst maschinell mit dem angegebenen Namen und Geburtsdatum aus dem Stammsatzbestand der DSRV ermittelt.

Die Kommunikation zwischen DSRV und Rentenversicherungsträgern erfolgt über den SPoC. Die übermittelten Daten werden beim Rentenversicherungsträger maschinell in die anhängigen Fachverfahren (Antragserfassung, Versorgungsausgleich) weitergereicht.

Abbildung 21: Elektronischer Versorgungsausgleich bei Ehescheidungen



Fremdauskünfteverfahren (eGVZ)

Seit dem 1. Januar 2013 haben Gerichtsvollzieher nach der Zivilprozessordnung (ZPO) und dem Sozialgesetzbuch (SGB) die Möglichkeit, von der Rentenversicherung Informationen über den Schuldner abzufragen, damit sie Forderungen erfolgreich eintreiben können, nämlich

- die derzeitige Anschrift der betroffenen Person
- sowie Namen, Vornamen oder Firma und Anschriften ihrer derzeitigen Arbeitgeber

Auf Grundlage dieser Informationen kann der Gläubiger dann vollstrecken, zum Beispiel durch eine Pfändung von Gehaltsforderungen oder Kontoguthaben des Schuldners.

Der Gerichtsvollzieher darf die Daten nur erheben, wenn er die gesetzlichen Anforderungen des § 74 a Absatz 2 SGB X erfüllt. Der Gerichtsvollzieher hat in seinem Ersuchen zu bestätigen, dass diese Voraussetzungen vorliegen.

Das Ersuchen und die Auskunft sind elektronisch zu übermitteln.

Für Verfahren bei den Behörden nach diesem Gesetzbuch werden grundsätzlich gem. § 64 Absatz 1 SGB X keine Gebühren und Auslagen erhoben. Abweichend davon erhalten die Träger der gesetzlichen Rentenversicherung für jede auf der Grundlage des § 74a Absatz 2 Satz 1 erteilte Auskunft eine Gebühr von 10,20 Euro.

Aufgrund der immer gleichen Anfrage- und Auskunftsformen eignete sich auch dieses Verfahren für eine elektronische Abbildung. Die Datenstelle erhielt den Auftrag, ein entsprechendes Verfahren für alle Rentenversicherungsträger zu entwickeln und zu betreiben.

Es wurden XJustiz Standards für Anfrage, Auskunft, Rechnung, Fehlermeldung, Prüffallmeldung etc. definiert. Die XJustiz Nachrichten werden über die EGVP-Infrastruktur versendet. Die eingehenden Datensätze werden vollautomatisiert verarbeitet, Fehlermeldungen und Prüffallmeldungen erzeugt und versendet sowie die Auskünfte und Rechnungen erstellt. Diese müssen noch von der Sachbearbeitung gesichtet und zum Versand freigegeben werden.

Die Auskünfte werden in der Regel noch am Tag der Anfrage, spätestens am folgenden Werktag dem anfragenden Gerichtsvollzieher zur Verfügung gestellt.

Der große Vorteil: Mit dem Einsatz dieser Anwendung bei der DSRV im Jahr 2015 konnte die relativ arbeitsintensive Sachbearbeitung beim Rentenversicherungsträger abgelöst werden. Lediglich in Prüffällen und bei der Forderungseintreibung entstehen manuelle Arbeitsvorgänge.

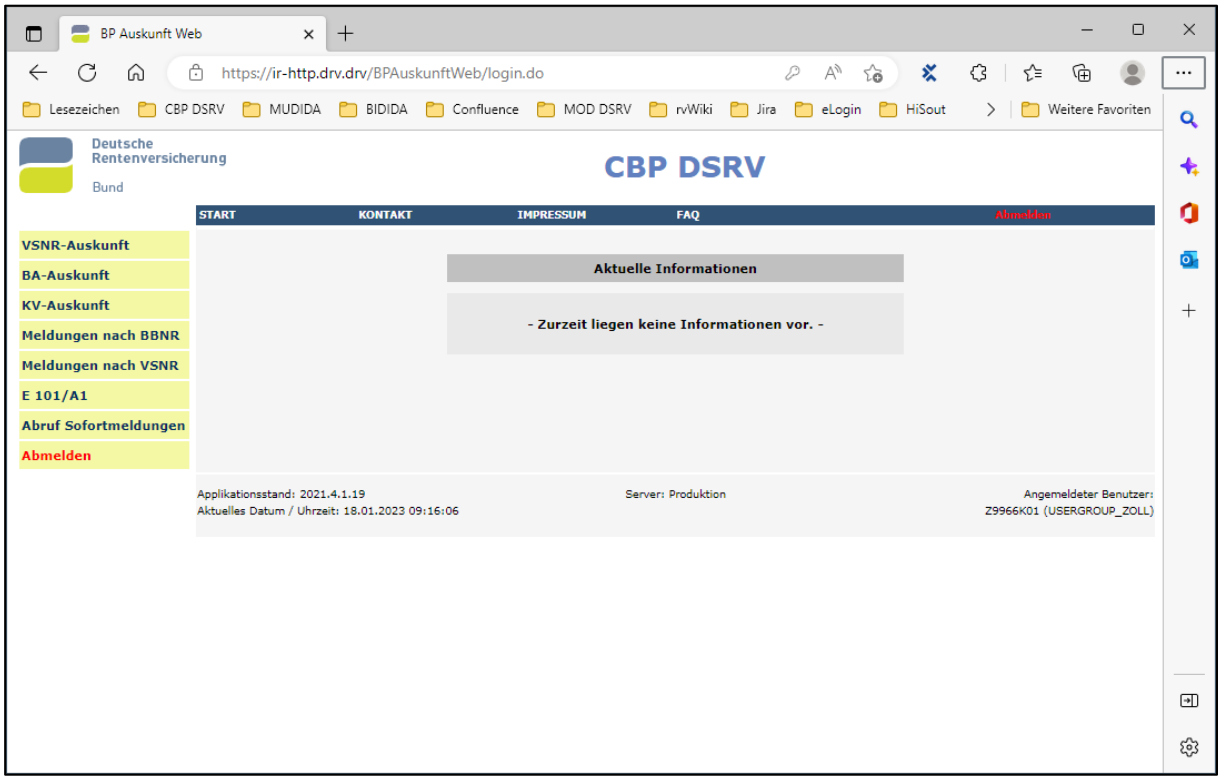
Im Jahr 2025 wurden 805.064 Anfragen von Gerichtsvollziehern elektronisch verarbeitet.

10.8 Zollauskunft (Beschäftigungszeiten/ A1 / Sofortmeldungen)

Den Behörden der Zollverwaltung wird von der DSRV Würzburg bereits seit längerem ein komfortabler Zugriff auf ihre geführten Dateien (Stammsatzdatei, Basisdatei, Betriebsdatei, KV-Beitragssatzdatei, A1 -Datei) und Verfahren gewährt. Die dort abgelegten Angaben zur Beschäftigung oder Entsendung unterstützen die Finanzkontrolle Schwarzarbeit (FKS) bei deren Recherchen und Vor-Ort-Prüfungen.

Die Ergebnisse helfen dabei auch den Sozialleistungsträgern, Beitragshinterziehungen aufzudecken. Als jüngster Teil der Auskunft wurden die Informationen zu den ab 1.1.2009 eingeführten Sofortmeldungen in bestimmten Wirtschaftsbereichen (siehe auch Kapitel 4.4) integriert. Die folgende Abbildung zeigt ein Bildschirmfoto dieser Anwendung.

Abbildung 22: Zollauskunft



10.9 Europäisches Online Auskunftsverfahren (EOA)

Mit dem „Europäischen Online-Auskunftsverfahren der Deutschen Rentenversicherung“ (EOA) können durch die zuständigen Träger eines EU-Mitgliedsstaates deutsche Versicherungsverläufe (E 505 DE) und deutsche Rentenbeträge des Rentenberechtigten online aufgerufen werden.

Abbildung 23: Europäisches Online Auskunftsverfahren (EOA)

Grundlage hierfür ist die jeweils zwischen den Trägern der Deutschen Rentenversicherung und dem ausländischen Rentenversicherungsträger getroffene Vereinbarung. Auf Grundlage dieser Vereinbarung können vom ausländischen Rentenversicherungsträger Benutzer benannt werden, um sie für das Verfahren zuzulassen. Die gemeldeten Benutzer erhalten

eine persönliche eindeutige achtstellige Benutzerkennung. Anfragen können sowohl mit einer deutschen Versicherungsnummer als auch mit in der Vereinbarung festgelegten persönlichen Daten des Versicherten erfolgen.

Bei der technischen Konzeption des EOA wurde darauf geachtet, dass einerseits vom ausländischen Rentenversicherungsträger so wenig technische Voraussetzungen wie möglich benötigt werden und andererseits dennoch ein sicheres Verfahren garantiert werden kann. Beim EOA handelt es sich um eine Webanwendung, die aus datenschutzrechtlichen Gründen vom ausländischen Rentenversicherungsträger über das europäische Netzwerk TESTA-NG (= Trans-European Services for Telematics between Administrations - New Generation) aufzurufen ist. Es handelt sich um ein Netz zur Kommunikation zwischen Verwaltungseinrichtungen in Europa. Dabei erfolgt eine verschlüsselte Übertragung der Daten. Einzige technische Voraussetzung für den Aufruf ist somit ein Internet-Browser am Arbeitsplatz des Benutzers, mit dem der Aufruf der Web-Adresse bei der DSRV über das Netzwerk TESTA-NG erfolgt. Die Daten werden „SSL (Secure Socket Layer) verschlüsselt“ übermittelt.

10.10 eBanking

Mit dem Verfahren eBanking bietet die Datenstelle der Rentenversicherung (DSRV) in Würzburg die sichere Abwicklung des Zahlungsverkehrs im Inland sowie im SEPA-Zahlungsraum für verschiedene RV-Träger an. Über das Verfahren eBanking werden u.a. Gehaltszahlungen, Zahlungen von Sozialversicherungsbeiträgen, Zahlungen von vermögenswirksamen Leistungen, Zahlungen im Rahmen der Rehabilitation, Beitragszahlungen der Krankenkassen, Zahlungen zur Riesterrente, Reisekosten sowie Beschaffung und Beihilfe abgewickelt. Nicht unter die eben genannten Zahlungsarten fallen hierbei die Rentenzahlungen, da diese an sich über den Postrentendienst abgewickelt werden. Allerdings müssen dem Postrentendienst die entsprechenden Mittel bereitgestellt werden. Dazu sind Gelder zu transferieren und/oder Konten aufzulösen. Dieser Part wird über die Banking-Software "UC eBanking Prime" vollzogen.

10.11 Digitale Rentenübersicht

Mit dem Inkrafttreten des Gesetzes zur Entwicklung und Einführung einer Digitalen Rentenübersicht (RentÜG) wurde die Deutsche Rentenversicherung Bund beauftragt, eine neue Organisationseinheit für die Entwicklung und den Betrieb dieses Portals Digitale Rentenübersicht zu schaffen – die Zentrale Stelle für die Digitale Rentenübersicht (ZfDR).

Das Portal mit Informationen zur gesetzlichen, betrieblichen und privaten Altersvorsorge auf der Grundlage des RentÜG soll Interessierten helfen, die finanzielle Absicherung im Rentenalter für sich einzuschätzen und sich intensiver mit der eigenen Altersvorsorge auseinanderzusetzen.

Im Einzelnen sind das:

- Renten aus Pflichtsystemen wie der gesetzlichen Rentenversicherung
- betriebliche Altersversorgung in der Privatwirtschaft (Direktversicherung, Direktzusage, Unterstützungskasse, Pensionskassen und Pensionsfonds),
- Zusatzversorgung des öffentlichen Dienstes,
- geförderte private Altersvorsorge (Riester-Renten, Rürup-Renten),
- private kapitalbildende Lebensversicherungen mit Auszahlungsbeginn ab dem 60. Lebensjahr,
- Altersvorsorge-Verträge in Form von Fondssparplänen mit Auszahlungsbeginn ab dem 60. Lebensjahr.

Interessierte Bürgerin und Bürger können unter www.rentenuebersicht.de nach einer Online-Authentifizierung im persönlichen Bereich des Portals ihre erworbenen

Altersvorsorgeansprüche bei den beteiligten Vorsorgeeinrichtungen digital abrufen. Diese werden in einem übersichtlichen Gesamtüberblick zusammengefasst. Die Digitale Rentenübersicht kann damit Grundlage für eine weitergehende Beratung sein, um etwaige Lücken in der Altersversorgung frühzeitig erkennen und handeln zu können.

Abbildung 24: Digitale Rentenübersicht

Ende 2023 startete das Portal Digitale Rentenübersicht in den Regelbetrieb. Nach und nach werden zusätzliche Anbieter von Altersvorsorge-Produkten angebunden und das Portal wird entlang der Interessen der Nutzenden weiterentwickelt.

Dieses Verfahren erfolgt über eine synchrone Kommunikation zwischen der ZfDR und den Rentenversicherungsträgern, so dass die Altersvorsorgeansprüche aus der gesetzlichen Rentenversicherung im Sinne einer Renteninformation möglichst sofort nach dem Datenabruf im Portal sichtbar sind. Für die Identifizierung einer Person werden die Identifikationsnummer nach § 139b der Abgabenordnung und das Geburtsdatum verwendet. Über diese Merkmale wird bei der DSRV die Versicherungsnummer aus dem Stammsatzbestand ermittelt, um die Anfrage an den zuständigen Rentenversicherungsträger zu adressieren. Die Kommunikation zwischen DSRV und Rentenversicherungsträgern erfolgt über die Dialogisierung.

Im Jahr 2023 wurden durch die Rentenversicherungsträger bereits 193.044 Auskünfte erteilt. Die bisherige Kommunikation auf dem Postweg zwischen den Rentenversicherungsträgern und den Versicherten, nämlich jährlicher Versand der Renteninformation an die Versicherten ab dem 27. Lebensjahr bleibt weiterhin bestehen.

10.11 Sicherheit bei Online-Services

Mit den Online-Services der Deutschen Rentenversicherung werden Sozialdaten erfasst, verarbeitet, gespeichert und gesendet. Dem ist bei der Implementierung der technischen Verfahren Rechnung zu tragen. Entsprechend müssen Risiko, Schutzziele und zu ergreifende Maßnahmen aufeinander abgestimmt werden.

10.11.1 Schutzziele und Risiko

Das größte Risiko bei den Online-Services der Rentenversicherung besteht vermutlich darin, Unbefugten Einsicht in Sozialdaten zu gewähren. Die folgende Tabelle bewertet die Risiken Vertraulichkeit, Datenintegrität und Verfügbarkeit hinsichtlich der Online-Services-Angebote:

Tabelle 2: Schutzbedarf bei den Online-Angeboten der Deutschen Rentenversicherung

Grundwert	**Schutz-bedarf**	**Begründung**
Vertraulich-keit	Hoch	Die ausgetauschten Daten sind Sozialdaten. Sie unterliegen dem § 35 SGB I (Sozialgeheimnis). Es ist Artikel 32 DSGVO (technische und organisatorische Maßnahmen) zum Schutz der Sozialdaten zu beachten. Unzulässige Datenerhebung, -verarbeitung und -nutzung führen zu Schadenersatzansprüchen nach Artikel 82 DSGVO. Der Imageschaden bei nicht sachgemäßer Erhebung, Verarbeitung und Nutzung ist als beträchtlich einzustufen.
Integrität	Hoch	Nichtautorisierte Veränderung gespeicherter oder übermittelter Daten und unbefugte Veränderung der Bestandsdaten der Rentenversicherung sind zu verhindern. Der Imageschaden bei nicht sachgemäßer Erhebung, Verarbeitung und Nutzung ist als beträchtlich einzustufen.
Verfügbarkeit	Normal	Ein Ausfall der Online-Dienstleitungen verursacht einen Imageschaden bei dem Kunden. Da alle Dienstleistungen aber nach wie vor per Telefon beziehungsweise Papier zur Verfügung stehen, kann darüber hinaus kein Schaden entstehen. Der Schutzbedarf für die Verfügbarkeit wird daher mit „gering bis mittel“ eingestuft.

10.11.2 Maßnahmen

Die Projektgruppe E-Government der Rentenversicherung hat für die Online-Services daher als wichtigste Sicherungsmaßnahme chipkartenbasierte starke Authentifizierungsverfahren und Verschlüsselungsverfahren als Standard der Rentenversicherung festgelegt:

Mit der **Verschlüsselungstechnik** (siehe auch Kapitel 11) wird die Vertraulichkeit gewährleistet. Die Übertragung von Informationen zwischen Browser und

Authentifizierungsserver wird mit einer Tiefe von 128 Bit verschlüsselt, d.h. es handelt sich quasi um eine Ende-zu-Ende-Verschlüsselung zwischen Absender und Empfänger.

Die nichtautorisierte Veränderung gespeicherter oder übermittelter Daten und unbefugte Veränderung der Bestandsdaten (Integrität) der Rentenversicherung wird beispielsweise durch die sichere Authentifizierung des (Privat-)Kunden verhindert. In den Nutzungsbedingungen ist dies festgelegt:

„Der ID Check der Deutschen Rentenversicherung

- *stellt Ihre Identität zweifelsfrei fest*
- *dient dem Schutz Ihres Steuer- und Sozialgeheimnisses.*

Nach der Identitätsprüfung erfolgt die Registrierung im Kundenportal. Dadurch stellen wir sicher, dass nur Sie auf Ihre persönlichen Daten zugreifen können. Im Kundenportal können Sie online Ihre persönlichen Informationen rund um die Rente abrufen und Online-Services nutzen.“

Jeder Privatkunde muss sich daher anhand einer **Signaturkarte, des Personalausweises, Aufenthaltstitels oder der Unionsbürgerkarte** „ausweisen“. Die entsprechenden Karten bieten durch die durchgeführte Evaluierung der Hard- und Software sowie des Kartenproduktionsprozesses ein Höchstmaß an Sicherheit, was die Technik der Chipkarte und die Organisation der Ausgabe (Registrierung, Personalisierung, Übergabe) angeht und erfüllt somit die hohen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) - siehe hierzu auch die technische Richtlinie des BSI TR-03107-1

Die Verfügbarkeit der Anwendung wird durch **redundante Server und Internetzugänge** sowie die Regelungen zu einem geordneten Rechenzentrumsbetrieb (zum Beispiel Sicherungsverfahren, Überwachung und Protokollierung) sichergestellt.

Außerdem gelten die Regelungen der Dienstanweisung zur Informationstechnik (DAIT) und ihrer Anhänge.

Im nun folgenden Kapitel wird auf weitere Verschlüsselungs- und Authentifizierungsverfahren sowie deren technischen Hintergrund etwas tiefer eingegangen.

ZUSAMMENFASSUNG

- In Kapitel 10 wurden die Möglichkeiten der Online-Verarbeitung und -Nutzung beschrieben, sowohl für den Versicherten als Online-Dienste wie für andere Behörden im Rahmen von eSolution. Neben einigen Beispielen haben wir auch kennen gelernt, welche sicherheitstechnischen Verfahren zur Absicherung der Online-Nutzung eingesetzt werden.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

48. Welche sind die wesentlichen Vorteile vom Online-Dienst „Anträge stellen“?

49. Nennen Sie weitere Online-Services der Rentenversicherung.

50. Warum ist die Einhaltung der datenschutzrechtlichen Vorgaben sowie ein sicheres Authentifizierungsverfahren für den Online-Zugriff auf das Versicherungskonto so bedeutend?

51. Welches ist die Zielgruppe für das Verfahren „eSolution“ der Deutschen Rentenversicherung?

11. Authentifizierung und Signatur, Datenverschlüsselung

LERNZIELE

- Sie kennen die gängigen Verfahren zur Authentifizierung an Datenverarbeitungsanlagen und Anwendungen.
- Sie kennen die Grundbegriffe der elektronischen Signatur und die möglichen Anwendungsgebiete.
- Sie können die Aufgaben eines Zertifizierungsdienste-Anbieters beschreiben.
- Sie kennen die Grundzüge von Verschlüsselungs- und Signaturverfahren

Der rasende Fortschritt in den letzten Jahren im Bereich der Telekommunikation und Informationstechnologie hat die kühnsten Erwartungen übertroffen und eröffnet ein breites Feld an neuen Anwendungsmöglichkeiten. Aber leider steigen damit auch die Risiken eines Missbrauchs von Daten und Systemen.

Bis vor wenigen Jahren war das Arbeiten in Netzwerken nur in nach außen abgeschlossen Systemen möglich, deshalb war die Frage nach der Sicherheit nicht besonders relevant, da ein Abhören entweder nur direkt oder im Bereich des Betreibers des Telefonnetzes möglich war. Heute ist dem Aspekt des unbefugten „Mithörens“ auf den teils offenen Leitungen viel höhere Aufmerksamkeit zu zollen. Wie kann man aber andererseits sicher sein, dass diejenige Person, mit der man kommuniziert, auch wirklich diejenige ist für die sie sich ausgibt?

Diese beiden Stichpunkte zeigen den erhöhten Bedarf an Sicherheit. Die Nutzung von Kryptografie kann die Umsetzung der erhöhten Sicherheitsanforderungen unterstützten.

Die Verwaltung der Benutzerkennungen und der zugehörigen Rechte in großen Institutionen ist mit erheblichem Aufwand verbunden. So muss jeder neue User angelegt und überprüft werden, es sind Maßnahmen vorzusehen, um Startpassworte einzurichten und diese müssen dem Nutzer sicher zugestellt werden. Nicht zu vernachlässigen sind ferner Regelungen, wie mit vergessenen oder ungültigen Passworten zu verfahren ist.

11.1 Authentifizierungsverfahren

Aus Gründen des Datenschutzes und der Datensicherheit soll der unberechtigte Zugang oder Zutritt zu Rechnern und gespeicherten Informationen verhindert werden. Hierzu dienen Konzepte, mit denen der Zugang sowie Berechtigungen in den Systemen geregelt werden Ein Berechtigter muss sich gegenüber dem System ausweisen. Diese **Authentifizierung** (Überprüfung) und Bestätigung einer behaupteten Identität, kann auf vielfältige Art geschehen.

Der Nutzer ist daraufhin für die Ausführung von Funktionen, entsprechend der für das Benutzerkonto im System hinterlegten Berechtigungen (in der Regel nach einem Rollenkonzept von System autorisiert.

Anmeldung mit Benutzerkennung und Passwort

Der Benutzer beispielsweise eines Personal Computers erhält eine Benutzerkennung (Benutzerkonto, User-ID, Account) und kennt sein geheimes Passwort. Durch die richtige Kombination von User-ID und Passwort authentisiert er sich gegenüber dem Rechner als berechtigter Nutzer aus und das System authentifiziert ihn durch die erfolgreiche Überprüfung des Passwortes.

Für die Bildung eines Passwortes gibt es vielfältige Regeln, die von System zu System variieren können. So werden bestimmte Mindestlängen ebenso vorgeschrieben wie die Verwendung von Ziffern und Sonderzeichen. Zumeist müssen Passworte nach einer bestimmten Zeit (zum Beispiel 30 Tage) geändert werden, um ein Ausspähen oder einen Verrat des Passwortes an Unbefugte zu erschweren. Benutzerkennung und Passwort gewähren eine sichere Authentifizierung nur so lange, wie das Passwort geheim bleibt; offen gelegte Passwörter öffnen dem Missbrauch Tür und Tor, da die Benutzerkennung selbst nicht geheim oder zumindest „erratbar“ ist. Jeder Nutzer ist daher zu einem sorgsamen Umgang mit seinen Passworten angehalten. Der Sicherheitsaspekt liegt bei der Vergabe von Passworten in erster Linie bei der Länge und Komplexität der Passwörter, insbesondere da auch sogenannte "Brute-Force-Angriffe" (systematisches Ausprobieren aller Passwortmöglichkeiten) zur Ermittlung von Passwörtern gibt.
Um die Ausnutzung eines gebrochenen Passwortes für verschiedene Einsatzbereiche zu vermeiden, sollte für jeden Zweck unterschiedliche Passwörter gewählt werden.

Allerdings benötigen unterschiedliche Systeme und Anwendungen meist auch unterschiedliche Benutzerkennungen und Passworte, was in der Praxis oft zu Problemen führen kann.

Biometrische Merkmale

Als weiteren Möglichkeit der Anmeldung können biometrische Daten zur Authentisierung verwendet werden. Hierzu werden eindeutige Merkmale der Person für den Zugriff auf Systeme verwendet, beispielsweise Fingerabdruck für Smartphones. Durch die Eindeutigkeit der Merkmale erfolgt die Zuordnung zu einer Benutzerkennung meistens durch das System selbst. Das Erkennen biometrischer Merkmale ist ein technisch komplexer Prozess, bei dem gewisse Toleranzen bei der Genauigkeit eingestellt werden müssen, um die Fehlerrate möglichst gering zu halten. (Verwechslungen mit ähnlichen Personen oder Ablehnungen der richtigen Personen, z.B. unrasiert, kalt-nasse Finger). Bei biometrischen Merkmalen besteht die Gefahr, dass biometrische Merkmale unbemerkt auf andere Träger kopiert werden. (Fotografie, falscher Finger mit z.B. von einem Glas kopiertem Fingerabdruck etc.).

Besitz

Der (physikalische) Besitz von Token beziehungsweise Erkennungsmarken können ebenfalls für eine Authentifizierung verwendet werden. Hierbei können Gegenstände sowie sogenannte Softtoken an die berechtigten Personen ausgegeben werden, um beispielsweise zu gesicherten Bereichen über Schleusen Zutritt zu erlangen.

Chipkarten und PIN

Um erhöhte Sicherheitsanforderungen zu erfüllen kann eine Kombination der vorangegangen Authentifizierungsfaktoren erforderlich sein, sogenannte Multifaktor Authentifizierungen (MFA) beziehungsweise Zweifaktorauthentifizierung (2FA). Eine Ausgestaltung dieses Prinzips „Besitz und Wissen“ stellt die Authentifizierung über eine **Chipkarte** dar. Zur Anmeldung an einem Datenverarbeitungssystem wird die Karte (Besitz) in einen Kartenleser eingeführt und ausgelesen. Durch die Eingabe einer PIN (Persönliche Identifikationsnummer) oder eines Passwortes (Wissen) bestätigt man wie bei der User-ID, dass man berechtigterweise diese Karte nutzt. Eine Verbesserung gegenüber dem Verfahren mit Kennung und Passwort ergibt sich hier aus dem physikalischen Besitz einer solchen Karte. Durch die Anmeldung mit Chipkarte können nach erfolgreicher Anmeldung die Berechtigungen des Nutzers aus dem System ausgelesen werden oder diese werden auf andere Art und Weise mit der Identität des Karteninhabers verknüpft. Ein Zugriff ist hier nur möglich, wenn der entsprechende Nutzer im System für die Aktion autorisiert ist.

Die Überprüfung der Nutzer, Ausgabe der Karte, Sperrdienste etc. müssen ebenfalls geregelt sein.

Einige Rentenversicherungsträger nutzen beispielsweise die Mitarbeiterkarten auch in der Funktion zur Authentifizierung gegenüber ihren IT-Systemen und haben die Arbeitsplatzrechner und Notebooks mit entsprechenden Kartenlesegeräten ausgestattet.

Personalausweis, elektronischer Aufenthaltstitel, Unionsbürgerkarte mit elektronischem Identitätsnachweis (eID)

Eine weithin nutzbare Möglichkeit der Authentifizierung bietet **Personalausweis mit eID**, der im November 2010 eingeführt wurde. Der Personalausweis beinhaltet unter anderem auch eine elektronische Identität (eID=elektronische Kennung), mit der sich ein Bürger gegenüber Behörden aber auch gegenüber privaten Diensten authentifizieren kann. Der Vorteil liegt dabei insbesondere darin, dass die staatlichen Meldebehörden die Zuordnung von elektronischer ID und Person übernehmen und nur geringer Verwaltungsaufwand beim Nutzer der Authentifizierungsfunktion anfällt. Firmen oder Behörden, welche die elektronische ID nutzen wollen, müssen allerdings vorher beim Bundesverwaltungsamt ein Berechtigungszertifikat zum Auslesen der Daten aus dem Personalausweis beantragen. Dabei wird festgelegt, welche Informationen aus dem Personalausweis ausgelesen werden dürfen. So reicht zum Beispiel für die Nutzung am Zigarettenautomaten das Datum „Alter“ aus, bei anderen Anwendungen werden hingegen die Namensinformationen benötigt. Nur die staatlichen Stellen wie Polizei und Grenzbehörden können das ebenfalls auf dem Personalausweis vorhandene Lichtbild nutzen.

Der **elektronische Aufenthaltstitel (eAufenthaltstitel)** mit zertifiziertem Chip wurde am 1. September 2011 eingeführt. Mit Einführung des „eAufenthaltstitel“ im Kreditkartenformat werden der bisherige Aufenthaltstitel (Klebeetikett), die Aufenthalts- und Daueraufenthaltskarte und der Ausweisersatz in Papierform abgelöst. Der elektronische Aufenthaltstitel besitzt einen kontaktlosen Chip im Karteninneren, auf dem die biometrischen Merkmale (Lichtbild und zwei Fingerabdrücke), Nebenbestimmungen (Auflagen) und die persönlichen Daten gespeichert sind. Zusätzlich enthält der Chip die Möglichkeit einen elektronischen Identitätsnachweis sowie eine qualifizierte elektronische Signatur zu nutzen. Zur Einführung des „eAufenthaltstitel“ wurden alle EU-Mitgliedstaaten verpflichtet. Grundlage hierfür sind die EU-Verordnungen Nummer 1030/2002 und Nummer 380/2008. Ziel ist es, die Aufenthaltstitel der Europäischen Union einheitlich zu gestalten und durch die Nutzung biometrischer Daten die Bindung zwischen Dokumenteninhaber und Dokument zu erhöhen und vor missbräuchlicher Nutzung zu schützen. Es wird für jeden Drittstaatsangehörigen ein eigener eAufenthaltstitel ausgestellt.

Abbildung 25: Muster für den Aufenthaltstitel

eID-Karte für Bürgerinnen und Bürger der EU und des EWR

Zum 1. Januar 2021 wurde die eID-Karte mit Online-Ausweisfunktion für Bürgerinnen und Bürger der Europäischen Union sowie Angehörige des Europäischen Wirtschaftsraums eingeführt.

Wie der Personalausweis und der elektronische Aufenthaltstitel enthält die neue Chipkarte die Online-Ausweisfunktion. Deren Inhaberinnen und Inhaber können sich damit sicher, einfach und auf hohem Vertrauensniveau online ausweisen und Behördengänge sowie Geschäftliches digital erledigen.

Abbildung 26: eID-Karte für Bürger*innen der EU

Im Kundenportal der Deutschen Rentenversicherung liegen zum Januar 2025 ca. 517.00 Registrierung mit den voran genannten Ausweisdokumenten vor.

11.2 Elektronische Signatur

Elektronische Signaturen sind Daten in elektronischer Form, die elektronischen Dokumenten beigefügt oder logisch mit ihnen verknüpft sind. Eine elektronische Signatur wird mit Hilfe des privaten Signatur-Schlüssels des Signaturschlüsselinhabers erzeugt und mit Hilfe seines öffentlichen Schlüssels geprüft. Siehe dazu auch Kapitel 11.3.Die elektronischen Signatur bestätigt,

- wer ein elektronisches Dokument signiert hat (Urheberschaft)

  und

- ob ein signiertes elektronisches Dokument manipuliert wurde (Integrität).

Die Signatur und ihre Verwendung

Die eIDAS-Verordnung (EU) Nummer 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/ 93/ EG regelt europaweit den Einsatz von Vertrauensdiensten und elektronischer Identifizierung. In der Verordnung ist auch beschrieben, dass Signaturen zwischen

- einfacher elektronischer Signatur,
- fortgeschrittener elektronischer Signatur
  und
- qualifizierter elektronischer Signatur unterschieden werden.

Die höchsten Sicherheitsanforderungen werden dabei an die qualifizierte elektronische Signatur gestellt. Aus der o.g. Verordnung ergeben sich die wesentlichen Anforderungen.

Qualifizierte elektronische Signaturen im Sinne der o.g. Verordnung werden nur dort benötigt, wo eine Rechtsvorschrift dies verlangt. Bestehen an Willenserklärungen beziehungsweise Handlungen im Verwaltungsverfahren keine besonderen Formerfordernisse, ist auch die elektronische Form keinen zusätzlichen Anforderungen unterworfen. Wird jedoch für die Rechtsverbindlichkeit eines Antrages, einer sonstigen Willenserklärung oder eines Verwaltungsaktes gesetzlich die Schriftform verlangt, muss das elektronische Dokument eine vergleichbare Sicherheit gewährleisten. Die Träger der Rentenversicherung benötigen qualifizierte elektronische Signaturen für einen rechtsverbindlichen elektronischen Daten- und Kommunikationsaustausch, zum Beispiel in internen Prozessen gemäß den Rechnungsvorschriften der Sozialversicherung sowie für die elektronische Archivierung von Unterlagen. Der weitaus überwiegende Teil der Bescheide der Rentenversicherung wird mit Hilfe der Datenverarbeitung erlassen. Nach § 33 Absatz 5 SGB X reicht für diese Bescheide eine fortgeschrittene elektronische Signatur aus, die nur die erlassende Behörde erkennen lassen muss.

Sowohl mit der qualifizierten elektronischen Signaturkarte als auch mit dem Personalausweis mit eID kann in Prozessen, bei denen eine formelle Unterschrift zum Abschluss eines rechtsverbindlichen Geschäftes/ Geschäftsvorgangs notwendig ist, wie beispielsweise zur Abgabe von Einwilligungserklärungen, die Änderung der Anschrift/ Bankverbindung oder die „Zugangseröffnung“ für die Einrichtung einer ausschließlich elektronisch basierten Kommunikation zwischen Versicherten und Rentenversicherungsträger die Anforderung der Schriftform erfüllt werden.

Trustcenter der Rentenversicherung

Vertrauensdienste-Anbieter (VDA) oder Trustcenter (trust = vertrauenswürdig) stellen elektronische Bescheinigungen (Zertifikate) über die Zuordnung sog. öffentlicher Schlüssel zu einer natürlichen Person aus, die im Zusammenhang mit der Anwendung der elektronischen Signatur, zur Verschlüsselung und zur signaturbasierten Authentisierung benötigt werden. Es handelt sich um besonders vertrauenswürdige Stellen, die vom Staat geprüft und zugelassen werden. Ein Trustcenter ist eher technisch organisatorisches Element. VDA sind gesetzlich geregelt (eIDAS, Vertrauensdienstegesetz (VDG), Vertrauensdienstverordnung(VDV)).

Zu den Aufgaben eines VDA gehört:

- Die Ausgabe von Chipkarten mit Schlüsselpaaren (privater / öffentlicher Schlüssel),
- die Personalisierung der Chipkarte,

- die Ausstellung von Attributzertifikaten
- die Kennzeichnung von Zertifikaten mit einer elektronischen Signatur,
- der Betrieb eines Verzeichnisdienstes zum Abruf und zur Prüfung der Zertifikate,
- der Betrieb eines Sperrdienstes und die Veröffentlichung von Sperrlisten.

Die Erzeugung von Schlüsseln und Zertifikaten sowie deren Verwendung zur Signatur oder zur Datenverschlüsselung sind Anwendungen der Kryptografie.

11.3 Datenverschlüsselung und –signierung

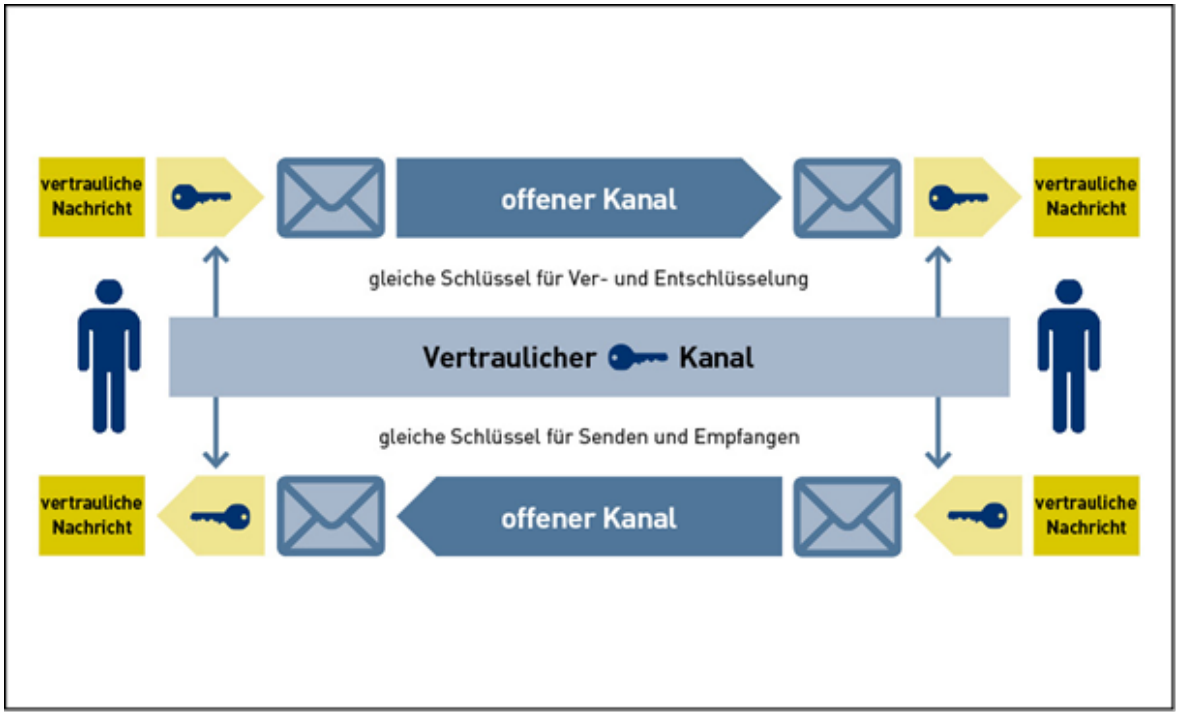
Die grundsätzliche Aufgabe der **Kryptografie** ist es, aus einem Klartext, den jeder lesen kann durch Chiffrierung (Verschlüsselung) einen Geheimtext zu machen, den nur noch solche
Personen lesen können, die Kenntnis von einem Geheimnis, nämlich dem Verschlüsselungsverfahren und dem eingesetzten Schlüssel haben.

Bei aktuellen symmetrischen und asymmetrischen Verschlüsselungsverfahren, auf die im Folgenden näher eingegangen wird, handelt es sich um Familien von parametrisierten Verfahren. Der ausgewählte Parameter wird auch Schlüssel genannt und muss von den Kommunikationspartner ganz oder teilweise geheim gehalten werden. Um zu gewährleisten, dass der Schlüssel nicht von Unbefugten mit Hilfe von Computern schnell herausgefunden werden kann, muss die Schlüssellänge groß genug sein. Bei heutigen Verschlüsselungsverfahren werden unterschiedliche mathematische Vorgehensweisen verwendet, vor allem die Primfaktorenzerlegung.

Symmetrische Verfahren

Beim symmetrischen Verschlüsselungsverfahren wird für das Ver- und das Entschlüsseln jeweils derselbe Schlüssel verwendet. Um zu gewährleisten, dass die Kommunikation zwischen A und B sicher ablaufen kann, darf der Schlüssel den beide Kommunikationspartnern nutzen, aber niemand anderem bekannt sein.

Abbildung 27: Schematischer Ablauf eines symmetrischen Verschlüsselungsverfahrens

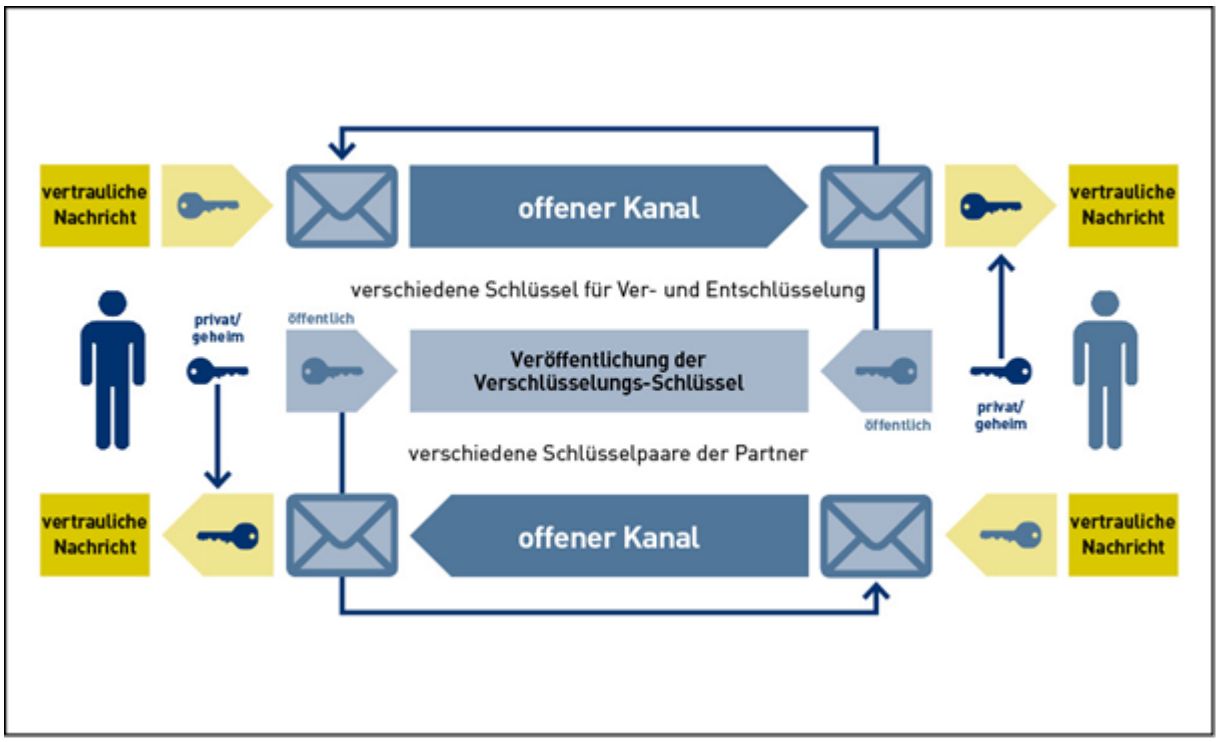


Bevor eine verschlüsselte Kommunikation stattfinden kann, müssen vorher ein oder mehrere Schlüssel generiert werden. Die Schlüsselgenerierung kann auf unterschiedliche Art und Weise von statten gehen: Entweder ausschließlich per Software oder mit Unterstützung durch Chipkarten, kryptografische Algorithmen mit Einbindung von Zufall. Nun muss der Schlüssel noch zum Kommunikationspartner gelangen, ohne dass eine nicht autorisierte Person den Schlüssel in seinen Besitz bringen kann. Die Schlüssel werden zum Beispiel per Post vor Beginn der Kommunikation ausgetauscht oder der Schlüssel, mit dem die Nachricht verschlüsselt wurde, wird selbst mit Hilfe eines Masterschlüssels verschlüsselt. Der Masterschlüssel muss allerdings wiederum vorher zwischen den Kommunikationspartnern ausgetauscht worden sein.

Asymmetrische Verfahren

Bei asymmetrischen Verschlüsselungsverfahren besitzt jeder Kommunikationspartner ein korrespondierendes Schlüsselpaar, das jeweils aus einem Public Key (Öffentlicher Schlüssel, allgemein bekannt) und einem Privat Key (Privater Schlüssel, geheim) besteht. Möchte nun A nach B eine Nachricht schicken, so benutzt er den Öffentlichen Schlüssel von B, der öffentlich zugänglich gemacht wird, um die Nachricht zu verschlüsseln. B benutzt nach Erhalt der verschlüsselten Nachricht seinen Privaten Schlüssel, um die Nachricht zu entschlüsseln.
Eine Entschlüsselung ist nur mit dem Gegenstück zum korrespondierenden öffentlichen Schlüssel möglich. Eine umgekehrte Kommunikation, also von B nach A funktioniert auf die gleiche Weise. Bei asymmetrischen Verschlüsselungsverfahren muss demnach jeder seinen Schlüssel öffentlich zugänglich machen.

Abbildung 28: Schematischer Ablauf eines asymmetrischen Verschlüsselungsverfahrens



Ein Nachteil der asymmetrischen Verschlüsselungsverfahren besteht darin, dass die höhere Komplexität bedeutend mehr Zeit für die Ver- und Entschlüsselung in Anspruch nimmt, wodurch sie für die Verschlüsselung großer Datenmengen eher ungeeignet sind. Deshalb verwendet man die asymmetrischen in Kombination mit den symmetrischen Verfahren beim sogenannten erwähnten Hybrid-Verfahren. Hierbei wird die eigentliche Nachricht mit einem symmetrischen Verfahren unleserlich gemacht. Der verwendete Schlüssel wird der Nachricht hinzugefügt und mit Hilfe des öffentlichen Schlüssels des Kommunikationspartners verschlüsselt, der dann mit seinem privaten Schlüssel den Vorgang wieder umkehren kann.

Ein großes Problem hierbei ist allerdings die Zuordnung des öffentlichen Schlüssels. Es muss gewährleistet werden, dass ein bestimmter öffentlicher Schlüssel einer Person 100-prozentig zugeordnet werden kann. Um diese Problematik bemühen sich die VDA, die wir im letzten Kapitel kennen gelernt haben.

Verschlüsseln und Signieren

Mit den Möglichkeiten der Verschlüsselung lässt sich der Inhalt einer Nachricht gegenüber Unbefugten verheimlichen. Verschlüsselungsverfahren eignen sich daher hervorragend zum Schutz von Informationen auf dem Transportweg, egal ob vollelektronisch über Telekommunikationsnetze oder auf physikalischen Datenträgern wie Bändern oder CDs.

Das Schutzziel Datenintegrität, also die Unverfälschtheit der Daten zwischen Absender und Empfänger (es hat zwischenzeitlich keine absichtliche oder unabsichtliche Veränderung der Daten stattgefunden) sowie die zweifelsfreie Kenntnis des Senders einer Nachricht (Authentizität) lassen sich mit Hilfe der Signatur feststellen. Die Signatur hat dabei keinen Einfluss auf die Lesbarkeit der Nachricht.

Eine Hashfunktion berechnet aus einem langen Text einen verhältnismäßig kurzen eindeutigen Wert (Hashwert), der die Eigenschaft hat, sich schon bei kleinsten Veränderungen im Text ebenfalls zu ändern. Beim Signieren wird über die gesamte Nachricht ein Hashwert gebildet, der mit dem privaten Schlüssel des Senders verschlüsselt

und zusammen mit der Nachricht übermittelt wird. Der Empfänger bildet anschließend ebenfalls den Hashwert über die Nachricht und vergleicht diesen mit dem übertragenen Wert, nachdem er diesen mit dem Public Key des Senders entschlüsselt hat. Stimmen sie überein, so ist erwiesen, dass die Nachricht auf dem Weg zum Empfänger nicht manipuliert worden ist (gleicher Hashwert) und dass der Absender mit dem Besitzer des öffentlichen Schlüssels übereinstimmt. Die Zuordnung Schlüssel Person wird durch ein Zertifikat einer vertrauenswürdigen dritten Instanz (VDA) durchgeführt.

Internet-Sicherheit

Auch im Internet werden mit diesen Mechanismen die Vertraulichkeit und Integrität von Daten sowie die Authentifizierung des Absenders sichergestellt. Verschlüsselung und Signatur erfolgen dabei über öffentliche und private Schlüsselpaare. Zertifikate, die für diesen Prozess ausgestellt werden, werden entweder von den Teilnehmern selbst erzeugt oder bei entsprechenden Sicherheitsanforderungen über Vertrauensdienste-Anbieter zur Verfügung gestellt. Der Einsatz von Verschlüsselungsverfahren wird im Internet meist über die Darstellung eines geschlossenen Schlosses angezeigt und oft als Verwendung von HTTPS (englisch: Hypertext Transfer Protocol Secure oder deutsch: sicheres Hypertext-Übertragungsprotokoll) oder SSL (englisch: Secure Sockets Layer - ein Netzwerkprotokoll zur sicheren Übertragung von Daten)
beschrieben.

Glücklicherweise wird dem Anwender heute viel von der technischen Handhabung dieser Sicherheitsverfahren abgenommen. Anders wäre eine dienstliche Nutzung von E-Mails kaum mehr möglich. So werden die Ver- und Entschlüsselung, die Bildung und Prüfung von Hashwerten oder die Signatur von den E-Mail-Systemen selbstständig erledigt, wenn sie einmal dafür eingerichtet sind. Auch erfolgt eine Leitungsverschlüsselung im Datenaustausch dann ohne Zutun eines Mitarbeiters vollautomatisch zwischen den beteiligten Routern oder speziellen Krypto-Boxen. Die notwendigen Schlüssel werden dabei sicher in den Geräten selbst gespeichert oder liegen extern auf Chipkarten, die nach Gebrauch verschlossen werden können.

Aufgrund des technischen Fortschritts sind die eingesetzten Verschlüsselungsverfahren und Keys jedoch nicht „für alle Ewigkeit“ als sicher anzusehen. Schnellere Rechner und leistungsfähigere Algorithmen führen dazu, dass die kryptografischen Verfahren durch bloßes Ausprobieren in „vertretbarer Zeit“ geknackt werden können. Daher sind die Schlüssel meist nur für drei Jahre gültig und müssen dann durch sicherere Verfahren und/ oder längere Schlüssel ersetzt werden.

ZUSAMMENFASSUNG

- In Kapitel 11 schließlich lernten Sie die Grundlagen der Datenverschlüsselung und der Signatur kennen. Sie haben gesehen, wie die Verschlüsselungstechnik eingesetzt wird, um die Vertraulichkeit, die Datenintegrität und die Authentizität der Information sicher zu stellen.

AUFGABEN ZUR SELBSTÜBERPRÜFUNG

52. Was ist das derzeit gebräuchlichste Authentifizierungsverfahren?

53. Was versteht man bei Authentifizierungsverfahren unter dem Prinzip „Besitz und Wissen“

54. Welche Prüfungen lassen sich mittels einer elektronischen Signatur durchführen?

55. Welche Aufgaben hat ein Vertrauensdienst-Anbieter?

56. Welchen gravierenden Nachteil haben asymmetrische Verschlüsselungsverfahren und wie versucht man diesen in der Praxis zu kompensieren.

Lösungen der Aufgaben zur Selbstüberprüfung

1. Durch die Art der elektronischen Bauelemente.

2. Die Dialogverarbeitung.

3. Die Übernahme der Daten auf Belege entfällt, es fallen keine Transportzeiten an, Medienbrüche entfallen, sofortige Ergebniskontrolle ist möglich, und es kann eine sofortige Fehlerbereinigung erfolgen.

4. Das Internet ist öffentlich, das Intranet dient der Kommunikation und Information innerhalb eines Unternehmens. Gemeinsam ist beiden die eingesetzte Technologie.

5. Das Rentenversicherungssystem (RV-System). Das Kernsystem aller Rentenversicherungsträger nennt sich rvDialog.

6. Personalverwaltung, Finanzverwaltung, Material- und Anlagenwirtschaft, Klinikverwaltungssystem.

7. Büro- und Kommunikationssysteme.

8. E-Mail und Informationsdatenbanken.

9. Vorteile: individuell, Kontrolle über Entwicklung, Wettbewerbsvorteile, teilweise Kostenersparnis; Nachteile: Aufbau von Spezialwissen notwendig, Komplexität, Neue Mitarbeiter/innen haben keine Vorerfahrungen mit dieser Software.

10. Die beiden Geschäftsführergremien sind die Arbeitsgruppe Informationstechnologie (AGIT) und der Fachausschuss für Finanzen und Organisation (FAFO).

11. Fachliche und Technische Entwicklungszentren (FEZ und TEZ).

12. Zukunftsfähigkeit, Herstellerunabhängigkeit, arbeitsteilige Entwicklung aller Träger, optimale Pflege, optimale Einsatzbedingungen.

13. Kosteneinsparungen, Synergieeffekte, Backup-Konzept,

14. Kommunikationsbedarf, Datenannahme und -abgabe, zentrale Datenhaltung, gemeinsame Hard- und Software.

15. In den §§ 145, 150 SGB VI sowie in § 36 DEÜV und weiteren Gesetzen.

16. Durch den Stammsatzbestand.

17. Bislang wurden rd. 149 Mio. Versicherungsnummern vergeben, davon sind ca. 24 Mio. aktiv versicherte Ausländer.

18. Vergabe der Versicherungsnummer, Eindeutigkeit der Versicherungsnummer gewährleisten, aktuellen Kontoführer feststellen, Führen der gesetzlich festgelegten Dateien (Stammsatz, Basisdatei für die Betriebsprüfung, Entsendebescheinigungen A1, Sofortmeldungen)

19. § 147 Absatz 1 und 2 SGB VI.

20. Die Versicherungsnummer ist ein für die gesamte Sozialversicherung einheitlich gültiger und absolut eindeutiger Ordnungsbegriff, der die Daten eines jeden Versicherten unverwechselbar kennzeichnet und sich von den Daten eines anderen Versicherten eindeutig unterscheidet.

21. Bereichsnummer, Geburtsdatum, Anfangsbuchstabe, Seriennummer, Prüfziffer.

22. Die Bereichsnummer.

23. Der DSRV.

24. Die Stammsatzdatei bei der DSRV.

25. Bei einer Mehrfachvergabe oder wenn die Versicherungsnummer fehlerhaft ist.

26. Durch Bildung eines eindeutigen Pseudonyms.

27. § 149 Absatz 1 SGB VI.

28. Die Daten, die zur Erfüllung der gesetzlichen Aufgaben erforderlich sind.

29. Persönliche Daten, rentenrechtlich relevante Zeiten, Leistungsdaten, Daten für den Versorgungsausgleich, Anerkennungsdaten, statistische Daten und sonstige Daten.

30. Persönliche Daten.

31. Aktueller Kontoführer.

32. Der Versicherungsträger, der bei der Vergabe durch die DSRV festgelegt wird (§ 127 Absatz 1 SGB VI)

33. Dauerkontoführung durch DRV KBS, Dauerkontoführung wegen Vertrag, Antragseingang.

34. Kontoanforderung, Kontoübermittlung, Quittung.

35. Plausibilitätsprüfungen, Querverbindungsprüfungen, Wartezeit- und Voraussetzungsprüfungen.

36. Verursachersatz.

37. DSRV und Einzugsstellen.

38. Die sofortige Auskunft für jeden Versicherten an jeder beliebigen RV-Auskunftstelle in Deutschland.

39. Versicherungsverläufe, Lückenhinweis, Rentenauskünfte „Erwerbsminderung“, Rentenauskünfte „Altersrente“, Auskünfte über den Beitragserstattungsanspruch.

40. Manuelle (Einzel-)Aufträge, maschinelle Auslösung und turnusmäßige Verarbeitung.

41. Papierausdrucke, Datensätze (zum Beispiel Zahlungsanweisungen), Daten zur Speicherung im Versicherungskonto sowie statistische Informationen.

42. Eine Folge von Einzeltätigkeiten, die schrittweise ausgeführt werden, um ein geschäftliches oder betriebliches Ziel zu erreichen.

43. Grafische Darstellung als Fluss- und Ablaufdiagramm.

44. Heute erfolgen einzelne Arbeitsschritte automatisiert; der Workflow übernimmt die komplette Prozesssteuerung.

45. Die Einführung eines Dokumentenmanagementsystems (elektronische Akte).

46. Medienbruchfreie Aktenführung, Kostenvorteile durch verringerten Personalbedarf (Archiv), Wegfall von Mietzins für Gebäude sowie den Wegfall von Transportkosten.

47. Erfassen (Scannen) – Speichern – Recherche – Ausgabe/ Anzeige.

48. Gespeicherte Daten sind nutzbar, Daten werden bereits in maschinell weiterverwertbarer Form erfasst und gespeichert, Prüfung auf Plausibilität und Vollständigkeit bereits bei der Eingabe.

49. Online-Services ”Versicherungsunterlagen anfordern”, ”Termine vereinbaren” und “Persönliche Daten ändern”.

50. Personenbezogene Daten/ Sozialdaten dürfen nur an den berechtigten Empfänger weitergegeben werden. Zur Sicherstellung dieser Identität kommen Signaturkarten und der Personalausweis/ elektronische Aufenthaltstitel mit eID zum Einsatz.

51. Behörden und Datenlieferanten (z.B. Krankenkassen, Bundesagentur für Arbeit).

52. Benutzerkennung und Passwort.

53. Zugangsverfahren mit zwei getrennten Komponenten, beispielsweise Chipkarte oder Benutzerkennung als Besitz und Kenntnis von PIN oder Passwort als geistiges Wissen.

54. Die Prüfung auf die Urheberschaft (Authentizität) sowie die Prüfung, ob ein elektronisches Dokument manipuliert wurde (Integrität).

55. Ausgabe der Chipkarten einschließlich Public und Private Key, Personalisierung der Karte, Ausstellung von Attributzertifikaten, Signatur von Zertifikaten mit der Signatur des Trustcenters, Betrieb eines Verzeichnisdienstes sowie eines Sperrdienstes.

56. Zu langsam bei großen Datenmengen; Kompensation durch Einsatz von Hybrid-verfahren.

Verzeichnis der Abbildungen und Tabellen

Abbildung 1: Gremienstruktur der DRV-IT 18
Abbildung 2: IT- Sicherheitsbeauftragter der DRV 23
Abbildung 3: Rechenzentrumsstandorte der Deutschen Rentenversicherung 25
Abbildung 4: EESSI Gesamtarchitektur 32
Abbildung 5: Die DSRV als Kommunikationspartner 34
Abbildung 6: Aufbau einer Versicherungsnummer 37
Abbildung 7: Schematischer Ablauf des Kontoaustausches 49
Abbildung 8: Fachliches Design von Geschäftsprozessen 72
Abbildung 9: Beispiele für UML-Diagramme und deren Zusammenspiel 73
Abbildung 10: Beispiel für ein Modellierungstool: ADONIS mit grafischer Darstellung 74
Abbildung 11: Workflow in der Minijob-Zentrale 78
Abbildung 12: Funktionsübersicht „Elektronische Archivierung“ 79
Abbildung 13: Struktur der digitalen Akte 81
Abbildung 14: Einstieg Kundenportal 85
Abbildung 15: ID Check zum Nutzen digitaler Angebote 85
Abbildung 16: ID Check der Deutschen Rentenversicherung 87
Abbildung 17: Das Kundenportal der Deutschen Rentenversicherung 88
Abbildung 18: Online-Service ohne Identifikation 89
Abbildung 19: Anforderung von Druckprodukten 90
Abbildung 20: Informationsseite zum Verfahren eSolution auf der Seite der DSRV (www.dsrv.info/esolution) 92
Abbildung 21: Elektronischer Versorgungsausgleich bei Ehescheidungen 97
Abbildung 22: Zollauskunft 99
Abbildung 23: Europäisches Online Auskunftsverfahren (EOA) 99
Abbildung 24: Digitale Rentenübersicht 101
Abbildung 25: Muster für den Aufenthaltstitel 107
Abbildung 26: eID-Karte für Bürger*innen der EU 107
Abbildung 27: Schematischer Ablauf eines symmetrischen Verschlüsselungsverfahrens 110
Abbildung 28: Schematischer Ablauf eines asymmetrischen Verschlüsselungsverfahrens 111

Tabelle 1: Stammsatzbestand am 1.1.2026 32
Tabelle 2: Schutzbedarf bei den Online-Angeboten der Deutschen Rentenversicherung 102

Verfügbare Titel der Studientext-Reihe

Nummer 1	Dietzel	Sozialversicherung
Nummer 2	Schindler	Versicherungspflicht
Nummer 3	Czok * Hillig	Beitrags- und Meldewesen
Nummer 4	Loukidou	Selbständige
Nummer 5	Rosenbusch	Versicherungsfreiheit
Nummer 6	Sibum	Freiwillige Versicherung
Nummer 7	Jungbauer	Nachversicherung
Nummer 8	Schulte	Wirksamkeit der Beitragszahlung
Nummer 9	Hiller	Beitragserstattung
Nummer 10	Raps	Anerkennung von Beitragszeiten
Nummer 11	Kühl	Fremdrentenrecht
Nummer 12	Prietzel	Leistungen zur Teilhabe
Nummer 13	Küppenbender	Übergangsgeld
Nummer 14	Böwing	Ergänzende und sonstige Leistungen, Zuzahlung
Nummer 15	Mellmann * Knobloch	Rentenantragsverfahren
Nummer 16	Lennecke * Limbeck	Renten wegen Alters
Nummer 17	Benen	Renten wegen verminderter Erwerbsfähigkeit
Nummer 18	Brettschneider	Renten wegen Todes
Nummer 19	Strotmann	Wartezeiten
Nummer 20	Begert	Rentenrechtliche Zeiten
Nummer 21	Beckwermert	Rentenberechnung
Nummer 22	Viergutz	Zusammentreffen von Renten und Einkommen
Nummer 23	Klüpfel	Versorgungsausgleich
Nummer 24	Gries	Pfändung, Abtretung, Aufrechnung von Renten
Nummer 25	Seliger-Hartmann * Steupert	Rentenzahlverfahren, Vorschüsse und Verzinsung
Nummer 26	Stempfhuber	Erstattungsansprüche der Leistungsträger
Nummer 27	Dopheide * Bartelt	Verwaltungsverfahren I (SGB I)
Nummer 28	Reinartz	Verwaltungsverfahren II (SGB X)
Nummer 29	Zepke	Krankenversicherung der Rentner
Nummer 30	Gutzler	Über- und zwischenstaatliches Recht, Auslandsrenten
Nummer 31	Ruder * Seeg	Datenverarbeitung in der Rentenversicherung

Nummer 32	Schulmeister	Datenschutz in der Rentenversicherung
Nummer 33	Brüßeler	Arbeits- und Dienstrecht
Nummer 34	Becker	Knappschaftsrecht I: Versicherung und Beitrag
Nummer 35	Stehr ∗ Böttcher	Knappschaftsrecht II: Leistungen
Nummer 36	Schmidt-Kühlewind	Sozialgerichtsgesetz
Nummer 37	-	Wird nicht mehr aufgelegt
Nummer 38	Jäger * Reich	Lern- und Arbeitstechniken
Nummer 39	Jäger * Reich	Kommunikation – Kooperation
Nummer 40	Tippelmann	Altersvorsorge

Impressum

1. Auflage 1993
30. Auflage 2026
Rechtsstand 01.01.2026

Autor*in Natalia Ruder, Michael Seeg
- Deutsche Rentenversicherung Bund
Fachgutachter*in Natalia Ruder, Michael Seeg
- Deutsche Rentenversicherung Bund

Herausgeber © Deutsche Rentenversicherung Bund
Personal, People & Development
Produktcenter Personalentwicklung
Prozesse, Standards und IT
Hohenzollerndamm 46/47
10704 Berlin

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.

Liebe Leser*innen außerhalb der Deutschen Rentenversicherung:

Für Auskünfte zu diesem und allen anderen fachlichen Themen rund um Versicherung, Rente, Reha und Altersvorsorge wenden Sie sich bitte an unsere Expert*innen am **Servicetelefon** der Deutschen Rentenversicherung unter:

0800 1000 4800 (Montag bis Donnerstag von 7:30 bis 19:30 Uhr, Freitag bis 15:30 Uhr)

Oder nehmen Sie auf anderem Wege Kontakt auf:

Kontakt | Deutsche Rentenversicherung (deutsche-rentenversicherung.de)