



Verbindliche Entscheidung des Bundesvorstandes der Deutschen Rentenversicherung Bund

Der Bundesvorstand der Deutschen Rentenversicherung Bund hat folgende verbindliche Entscheidung getroffen:

Die Anwendung des Branchenspezifischen Sicherheitsstandards B3S DRV (Anlage) wird für alle Träger der Deutschen Rentenversicherung verbindlich beschlossen.

Es wird verbindlich beschlossen, dass die Steuerung und Koordination der DRV übergreifenden Aufgaben zur IT-Sicherheit und die Nachweispflichten im Rahmen der BSI-KritisV Aufgaben des bestellten IT-Sicherheitsbeauftragten der DRV sind.

Die Entscheidung beruht auf § 138 Abs. 1 Satz 2 Nr. 6, Abs. 2 Satz 1 SGB VI, § 51 Abs. 2 Nr. 6 der Satzung der Deutschen Rentenversicherung Bund. Die Zuständigkeit des Bundesvorstandes ergibt sich aus § 138 Abs. 2 Satz 2 SGB VI, § 53 Abs. 2 der Satzung der Deutschen Rentenversicherung Bund i. V. m. dem Beschluss der Vertreterversammlung (heute: Bundesvertreterversammlung) über die Delegation von Aufgaben vom 1. Oktober 2005.

Die Entscheidung wird mit der Veröffentlichung im Amtlichen Mitteilungsblatt der Deutschen Rentenversicherung Bund verbindlich.

Berlin, 14. Mai 2020

Annelie Buntenbach

Alexander Gunkel

Anlage: B3S DRV

- unbesetzt -

Deutsche Rentenversicherung

Branchenspezifischer Sicherheitsstandard

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 2 von 40
--	---	-----------------

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	3
2	Einleitung	6
3	Teil 1: Geltungsbereich, Gefährdungs- und Risikoanalyse	8
3.1	Geltungsbereich.....	8
3.1.1	Eingrenzung der kritischen Dienstleistung.....	9
3.1.2	Abgrenzung	9
3.1.3	Extern erbrachte Leistungen	10
3.1.4	Gesetzlicher Rahmen.....	10
3.1.4.1	KRITIS-Betrachtung gemäß BSIG und BSI-KritisV.....	10
3.1.4.2	Zuständigkeiten und Aufgaben der DRV gemäß Sozialgesetzbuch.....	11
3.2	Schutzziele	11
3.2.1	Leistungssystem	14
3.2.2	Schnittstellen zum Auszahlungssystem.....	14
3.2.3	Prozessbeschreibung.....	15
3.3	Branchenspezifische Gefährdungslage.....	16
3.3.1	All-Gefahrenansatz.....	16
3.3.2	Branchenspezifische Relevanz von Bedrohungen und Schwachstellen.....	16
3.3.3	Benennung der maßgeblichen Gefährdungen	17
3.4	Risikomanagement	18
3.4.1	Geeignete Behandlung aller für die kDL relevanten Risiken.....	18
3.4.2	Beschränkung der Behandlungsalternativen für Risiken	18
3.4.3	Berücksichtigung von Abhängigkeiten bei der Risikoanalyse	19
3.4.4	Berücksichtigung der allgemeinen Gefährdungslage.....	19
3.4.5	Berücksichtigung der branchenspezifischen Gefährdungslage.....	20
3.5	Fortschreibung des B3S	20

4	Teil 2: Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen	21
4.1	Informationssicherheitsmanagementsystem (ISMS).....	21
4.2	Erstellung von IT-Sicherheitskonzepten	23
4.2.1	Basis-IT-Sicherheitskonzepte.....	23
4.2.2	IT-Verfahrenssicherheitskonzepte	23
4.3	Asset Management.....	24
4.4	Risikoanalysemethoden.....	24
4.5	Business Continuity Management (BCM) für kritische Dienstleistungen.....	24
4.6	Resiliente Architektur	25
4.7	Branchenspezifische Technik.....	25
4.8	Technische Informationssicherheit.....	25
4.9	Personelle und organisatorische Sicherheit	26
4.10	Bauliche und physische Sicherheit.....	26
4.11	Vorfallerkennung und –bearbeitung.....	27
4.12	Überprüfung	28
4.13	Externe Informationsversorgung und Unterstützung	28
4.14	Externe Dienstleister.....	29
5	Teil 3: Nachweisbarkeit der Umsetzung (Prüfungen)	30
5.1	Kurzprüfungen	31
5.2	Querschnittsprüfungen.....	31
5.3	Partialprüfungen	32
5.4	Einsichtnahme durch das BSI.....	32
6	Anhang A: Maßnahmen zur Behandlung von Bedrohungen und Schwachstellen.....	33
6.1	Mögliche Bedrohungen	33
6.2	Mögliche Schwachstellen	34
6.3	Richtlinien und damit verbundene Maßnahmen zur Behandlung von Bedrohungen und Schwachstellen:	34

7	Anhang B: Verzeichnisse	36
7.1	Abkürzungen	36
7.2	Abbildungen	38
7.3	Tabellen	38
7.4	Referenzierte Dokumente	38
7.5	Anlagen	40

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 6 von 40
--	---	------------------------

2 Einleitung

Die Datenverarbeitung und der Einsatz vielfältiger Informations- und Kommunikationstechniken spielen eine Schlüsselrolle für die Aufgabenerfüllung in der Deutschen Rentenversicherung (DRV). Wichtig ist insbesondere die rechtmäßige, zuverlässige und korrekte Verarbeitung der Daten. Die zur Datenverarbeitung genutzten und bereitgestellten Einrichtungen bedürfen daher eines Schutzes, der dieser Bedeutung gerecht wird.

Die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) definiert kritische Infrastrukturen zur Versorgung der Bevölkerung mit kritischen Dienstleistungen. Hierzu zählen aufgrund des gesetzlichen Auftrags das Leistungssystem und das Auszahlungssystem der gesetzlichen Rentenversicherung. Das Leistungssystem der DRV wird von ihr selbst entwickelt, gepflegt und betrieben.

Die DRV bringt monatlich ca. 25,5 Millionen Renten zur Auszahlung. Diese belaufen sich pro Monat auf eine Summe von 22,5 Milliarden Euro. Ferner verwaltet die DRV aktuell 102 Millionen aktive Versicherungskonten. Ferner werden monatlich Meldungen von über 30 Millionen Beitragszahlern entgegen genommen und in die Versicherungskonten gespeichert. Durch ihren gesetzlichen Auftrag zählt die DRV zu den kritischen Infrastrukturen (KRITIS) in Deutschland.

Das Auszahlungssystem der allgemeinen Rentenversicherung (ca. 97% der Renten) wird vom Rentenservice der Deutschen Post AG (RS) betrieben. Über technische und organisatorische Schnittstellen sind diese miteinander verbunden.

Das Auszahlungssystem der Knappschaftsrenten im Inland (ca. 3% der Renten) wird von der DRV Knappschaft-Bahn-See (KBS) eigenständig betrieben.

Gemäß § 8a (2) S. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) können Betreiber kritischer Infrastrukturen branchenspezifische Sicherheitsstandards (B3S) zur Umsetzung der Anforderungen nach § 8a (1) BSIG vorschlagen.

Dieses Dokument stellt den branchenspezifischen Sicherheitsstandard der Deutschen Rentenversicherung (B3S DRV) dar und operationalisiert die gesetzlichen Anforderungen an die Betreiber der kritischen Infrastruktur im Bereich der DRV.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 7 von 40
--	---	------------------------

Die Struktur dieses Dokumentes ist an die „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ in der Version 1.0 vom 01.12.2017 angelehnt.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 8 von 40
--	---	------------------------

3 Teil 1: Geltungsbereich, Gefährdungs- und Risikoanalyse

3.1 Geltungsbereich

Die DRV wurde im Rahmen der BSI-KritisV dem Sektor Finanz- und Versicherungswesen zugeordnet. Der Geltungsbereich dieses B3S umfasst die Versicherungsleistungen als kritische Dienstleistungen (kDL) nach BSI-KritisV §7 Abs. 1, Nr. 5 i.V. mit Abs. 6 und Abs. 7.

Die relevanten Anlagenkategorien ergeben sich aus dem Anhang 6, Teil 1 Abs. 1 zur BSI-KritisV:

- Buchstabe v: Leistungssystem der gesetzlichen Rentenversicherung als integriertes Anwendungssystem zur Erfassung, Prüfung und Berechnung von sozialversicherungsrechtlichen Entgeltersatzleistungen. Der Schwellwert beträgt 500 000 Leistungsfälle pro Jahr gem. BSI-KritisV, Anhang 6, Teil 3, Nr. 5.1.5.
- Buchstabe y: Auszahlungssystem als System zur Auszahlung der Versicherungsleistung an den Zahlungsempfänger. Der Schwellwert beträgt 500 000 Leistungsfälle pro Jahr gem. BSI-KritisV, Anhang 6, Teil 3, Nr. 5.1.9.

Das Auszahlungssystem der allgemeinen Rentenversicherung betreibt der Rentenservice Deutsche Post AG (Auszahlung der Renten an die Rentenempfänger). Seitens der DRV erfolgt ein Datenaustausch, um den Zahlbestand aktuell zu halten und es werden die finanziellen Mittel zur Auszahlung der Renten bereit gestellt (technische und organisatorische Schnittstellen).

Die DRV umfasst

- die 16 Rentenversicherungsträger (RVTR):
 - DRV Bund,
 - DRV Knappschaft-Bahn-See (KBS) und
 - die Regionalträger,
- die Datenstelle der Rentenversicherung (DSRV) sowie
- die beiden IT-Dienstleister RZW GmbH und NOW IT GmbH.

Der Geltungsbereich umfasst erbrachte Leistungen zur Aufrechterhaltung der kritischen Dienstleistung, die sowohl von der DRV selbst als auch von Dritten erbracht werden.

Als technische Anlagen der kritischen Dienstleistung werden die Infrastruktur (Gebäude, technische Infrastruktur, IT-Systeme) der Rechenzentren (RZ) der DRV (RZW-GmbH, NOW-IT, RZ DRV-Bund (Berlin), RZ DRV Berlin-Brandenburg, RZ DRV KBS und RZ DRV Oldenburg-Bremen) sowie das gemeinsame Netz der DRV (DRV-WAN) und die DSRV definiert.

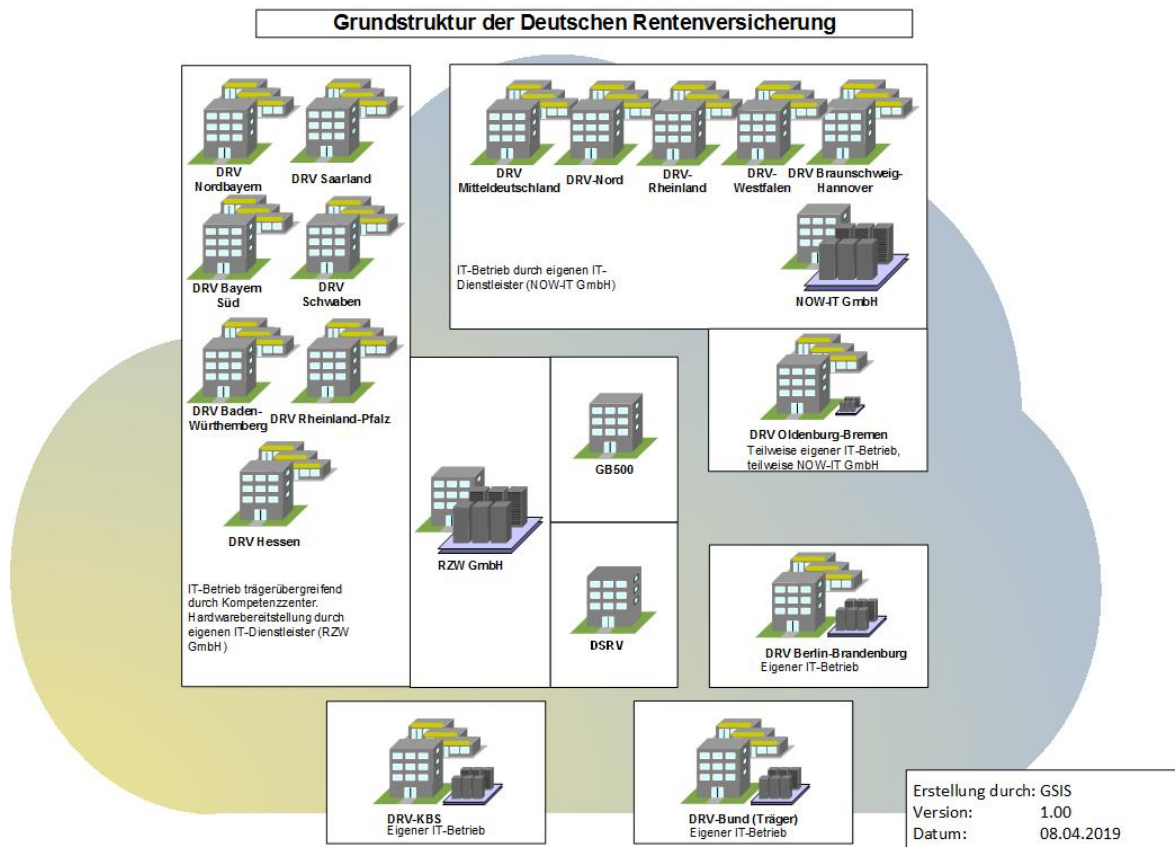


Abbildung 1 Technische Anlagen

3.1.1 Eingrenzung der kritischen Dienstleistung

Die Gültigkeit des B3S erstreckt sich zum einen auf das Leistungssystem der DRV und die Teile der Anlagen, um dieses zu betreiben (siehe 3.2.1).

Ferner ist, bezogen auf das Auszahlungssystem, der Datenaustausch mit dem RS und die Bereitstellung der Gelder zur Auszahlung der Renten Bestandteil der kritischen Dienstleistung (siehe 3.2.2).

3.1.2 Abgrenzung

Die Träger der allgemeinen Rentenversicherung lassen die laufenden Geldleistungen gem. §119 Abs. 1 S.1 SGB VI durch den Rentenservice Deutsche Post AG (RS) auszahlen. Die von der DRV sicherheitstechnisch zu betrachtende Anlagenkategorie „Auszahlungssystem“ für die Renten der allgemeinen

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 10 von 40
--	---	-------------------------

Rentenversicherung endet somit mit der Informations- bzw. Liquiditätsbereitstellung bezüglich der monatlich zu zahlenden Renten an den RS. Die technischen und organisatorischen Schnittstellen zwischen der DRV und dem RS werden als Grenze des Geltungsbereichs für den B3S sowie die entsprechenden Prüfungen festgelegt.

Das Auszahlungssystem der knappschaftlichen Rentenversicherung für Renten im Inland wird einzig durch die DRV KBS in Eigenverantwortung betrieben. Es ist daher nicht Gegenstand des B3S.

Darüber hinaus werden die zur Auszahlung der Renten erforderlichen Bereitstellungsprozesse der Bundeszuschüsse und der Leistungen der Bundesagentur für Arbeit nicht betrachtet, da diese außerhalb der Verantwortung der DRV liegen.

Ebenso werden die im Rahmen des Auszahlungsprozesses involvierten Kreditinstitute sowie deren IT-Infrastruktur und Prozesse nicht betrachtet.

3.1.3 Extern erbrachte Leistungen

Für extern erbrachte Leistungen durch Dienstleister zur Aufrechterhaltung der kDL gelten die Sicherheitsanforderungen, die gemäß Kapitel 4.14 an Dritte gestellt werden. Die Gesamtverantwortung verbleibt jedoch bei der DRV.

3.1.4 Gesetzlicher Rahmen

3.1.4.1 KRITIS-Betrachtung gemäß BSIG und BSI-KritisV

Dieser B3S berücksichtigt die gesetzlichen Anforderungen des BSIG i.V.m. der BSI-KritisV.

Danach sind angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.

Gemäß Anhang 6, Teil 1, Nummer 1, Buchstabe v und y der BSI-KritisV sind die nachfolgenden kritischen Anlagen relevant:

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 11 von 40
--	---	------------------

- Leistungssystem der Sozialversicherungsträger der gesetzlichen Renten-, Unfall- und Arbeitslosenversicherung
- Auszahlungssystem

3.1.4.2 Zuständigkeiten und Aufgaben der DRV gemäß Sozialgesetzbuch

Die Zuständigkeiten und Aufgaben der DRV sind in den Sozialgesetzbüchern (SGB) beschrieben:

- SGB I, § 12: Zuständigkeit für die Sozialleistungen,
- SGB IV, § 29: Rechtsstellung der Träger,
- SGB IV, § 90: Aufsicht über die Versicherungsträger,
- SGB VI, § 118: Fälligkeit und Auszahlung der Leistungen,
- SGB VI, § 119: Auszahlung über die Deutsche Post,
- SGB VI, § 138: Grundsatz- und Querschnittsaufgaben der DRV Bund,
- SGB VI, § 145: Aufgaben der Datenstelle der Rentenversicherung,
- SGB VI, § 149: Führen der Versicherungskonten,
- SGB VI, § 151a: Antragstellung im automatisierten Verfahren beim VA,
- SGB VI, § 153: Umlageverfahren,
- SGB X, § 79: Einrichtung automatisierter Verfahren auf Abruf,
- SGB X, § 80: Verarbeitung von Sozialdaten im Auftrag.

3.2 Schutzziele

Wesentliches Ziel des BSIG ist die Sicherstellung von existenzsichernden Leistungen für die Bevölkerung. Daraus leitet sich die Forderung ab, dass die IT-Systeme, Komponenten und Prozesse, mit denen solche kritischen Dienstleistungen erbracht werden, auf dem aktuellen technischen und organisatorischen Stand sein müssen, insbesondere zur Sicherstellung der Verfügbarkeit der Dienstleistung sowie der Authentizität, Integrität und der Vertraulichkeit der verarbeiteten Daten.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 12 von 40
------------------------------------	---	-------------------------

Das höchst zu schützende Gut der Deutschen Rentenversicherung (DRV) sind die Versicherungskonten und der Stammsatzdatenbestand. Diese bilden die elementare Grundlage für die Leistungserbringung der Rentenversicherung. Daher sind die Versicherungskonten und der Stammsatzdatenbestand – unabhängig von den jeweiligen Geschäftsprozessen – in besonderem Maße zu schützen.

Die in Tabelle 1 aufgeführten IT-Systeme, Komponenten und Prozesse wurden als elementare Bestandteile zur Erbringung der kDL identifiziert und bewertet. Diese werden hinsichtlich des Schutzbedarfs gem. BSI-Grundschatz bewertet. Diese Betrachtung wird ergänzt um eine Eingrenzung zur Sicherstellung der kritischen Dienstleistung. Diese weicht von der Betrachtung nach BSI-Grundschatz ab, da nicht der Schaden für das Unternehmen bewertet wird, sondern ausschließlich die Sicherstellung der Dienstleistung für die Bevölkerung. Als kritische Schadschwelle für die Verfügbarkeit wird ein Prozent der Renten (ca. 250.000 Fälle) angenommen.

- Der Schutzbedarf zu den Schutzziele „Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität“ ergibt sich aus der DRV-Richtlinie „Schutzziele und Schutzbedarf“ basierend auf dem BSI-Grundschatz und spiegelt den Schutzbedarf für den Normalbetrieb wieder.
- Das Schutzziel „Authentizität“ ist ein Teilbereich der Integrität und wird im diesem Rahmen berücksichtigt.

Schutzbedarf aus „KRITIS-Sicht“

- Der Schutzbedarf zu dem Schutzziel „Verfügbarkeit aus KRITIS-Sicht“ ergibt sich aus der Bewertung unter dem Aspekt der Sicherstellung der Versicherungsleistung.
Daraus ergeben sich teilweise andere Anforderungen an die Verfügbarkeit, da z.B. auch ein längerer Ausfall des Leistungssystems nicht zu einem Ausfall der Versicherungsleistung, d.h. der Auszahlung der Renten führt.
- Der Schutzbedarf zum Schutzziel „Reputation“ ergibt sich aus der Bewertung des Ansehens der DRV in der Öffentlichkeit sowie der Stimmung in der Bevölkerung bzgl. Sicherstellung der Rentenzahlungen. Diese Schutzbedarfseinordnung orientiert sich an der KRITIS-Sektorstudie „Finanz- und Versicherungswesen“ (2015) des BSI. Bewertet wird die Schadenskategorie „Psychologische Wirkung auf die Gesellschaft“ nach folgenden Kriterien:
 - Normal: hier nicht relevant
 - Hoch: Deutliche Beunruhigung großer Bevölkerungsteile
 - Sehr hoch: Tendenz zur „Massenhysterie“

IT-System, Komponente, Prozess	Beschreibung	BSI-Grundsicherheits-Ziele			Verfügbarkeit aus KRITIS- Sicht	Reputation
		Vertraulichkeit	Integrität	Verfügbarkeit		
DRV WAN	Das gemeinsame Netz der DRV	hoch	hoch	hoch	normal*	normal
Basis-IT-Infrastruktur	bezogen auf die RV-Träger, deren IT-Dienstleister und DSRV	hoch	hoch	hoch	normal*	hoch
Leistungssystem der DRV	bestehend aus rvDialog, rvPuR und rvArchiv	hoch	hoch	normal	normal*	hoch
DSRV-Verfahren	bestehend aus eAntrag, DEÜV und Stammsatz	normal	hoch	hoch	normal*	normal
Verfahren zur Unterstützung des Auszahlungssystems	bestehend aus eBanking, Rentenzahlverfahren	hoch	hoch	normal	normal*	normal
Liquiditätsbereitstellungsprozess	Organisatorischer Prozess zur Bereitstellung der Mittel für den RS	normal	hoch	Grds. normal, am Auszahlungstag sehr hoch**	Grds. normal, am Auszahlungstag sehr hoch**	hoch

* Überschreiten der Schadschwelle 1% Neurenten (nach ca. 8 Wochen).

** Ein Ausfall dieser Systeme am Zahltag kann dazu führen, dass dem RS nicht ausreichend Finanzmittel zur Auszahlung aller Renten zur Verfügung stehen und somit nur ein Teil der Renten ausgezahlt werden kann.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 14 von 40
--	---	-------------------------

Tabelle 1: Schutzbedarf

Der B3S bezieht sich auf die nachfolgend aufgeführten IT-Systeme, die zum Betrieb der kritischen Anlagen „Leistungssystem“ und „Schnittstellen zum Auszahlungssystem“ relevant sind.

Nicht betriebsrelevant sind

- IT-Systeme, die den Betrieb der kritischen Dienstleistung nicht direkt beeinflussen können oder deren Ausfall keine relevante Auswirkung auf den Betrieb hat, sowie
- Netzanbindungen, soweit diese nicht von den betriebsrelevanten Systemen genutzt werden.

3.2.1 Leistungssystem

Die betriebsrelevanten Verfahren und IT-Systeme einschließlich der davon genutzten Infrastrukturen und Netzwerke zum Betrieb der kritischen Anlage „Leistungssystem“ sind

- Verfahren des Programmsystems rvSystem:
 - rvDialog (Kernverfahren der Leistungsabteilung),
 - rvPuR (Frontend für digitale Akten) und
 - rvArchiv (digitales Archiv für Akten),
- Rentenzahlverfahren - Datenaustausch,
- Stammsatzdatei der Datenstelle (DSRV),
- DEÜV-Verfahren (Meldewesen zu Beiträgen und Zeiten n. §§ 28a bis 28c SGB IV),
- eAntrag (Verfahren zur Rentenantragsstellung).

3.2.2 Schnittstellen zum Auszahlungssystem

Im Bereich „Auszahlungssystem“ sind die Prozesse zur Bereitstellung der Finanzmittel an den RS für alle Rentenzahlungen mit Ausnahme der Zahlung der knappschaftlichen Rentenversicherung ins Inland (ca. 97% der Rentenzahlungen) zu berücksichtigen. Dabei handelt es sich um konsolidierte Zahldaten der RVTR und nicht um personenbezogene Daten bzw. Sozialdaten.

Die betriebsrelevanten IT-Systeme einschließlich der davon genutzten Infrastrukturen und Netzwerke zur Bereitstellung der Finanzmittel an die RS am Zahltag sind

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 15 von 40
--	---	-------------------------

- das zentrale Banking-System zur Ausführung von Eilüberweisungen „UC eBanking prime“ (e-Banking) sowie
- die Standard-Kommunikationsmittel Fax und Telefon, insbesondere bei der DRV Bund als koordinierende Stelle.

3.2.3 Prozessbeschreibung

Die nachfolgende Zusammenfassung gibt einen Überblick über die Prozesse zum Leistungs- und Auszahlungssystem.

- Meldung der Arbeitgeber an die DRV

Die Arbeitgeber melden über 18 Datenannahmestellen der Krankenkassen nach dem „Meldeverfahren nach der Datenerfassungs- und -übermittlungsverordnung“ (DEÜV) an die DSRV u.a. die Beitragszeiten. Die Beiträge selbst werden über die Krankenkassen als gesetzliche Einzugsstellen mittels Verteilschlüssel an die RVTR gezahlt.

- Weitergabe von Meldungen über die DSRV

Die DSRV ermittelt über die Sozialversicherungsnummer für jede Meldung über die Stammsatzdatei den kontoführenden RVTR und leitet die Information weiter. Dieser verarbeitet die Informationen und speichert diese jeweils im Versicherungskonto.

- Stellen von Rentenanträgen

Grundsätzlich werden die Rentenanträge bei den Auskunfts- und Beratungsstellen der DRV sowie bei den Gemeinde- und Versicherungsämtern gestellt. Hierzu stellt die DRV das zentrale Verfahren eAntrag zur Verfügung. Über dieses Verfahren werden die Rentenanträge an die DSRV weitergeleitet. Die DSRV leitet wiederum die Anträge an die jeweils kontoführenden RVTR weiter.

- Leistungssysteme (rvDialog)

Mittels des Verfahrens „rvDialog“ wird der jeweilige Antrag, der Anspruch sowie die Rentenhöhe geprüft, ermittelt und ggf. zur Auszahlung angewiesen. Ergänzend steht das Verfahren „rvPuR“ (inkl. „rvArchiv“) zur Verfügung, über das die elektronischen Akten gehalten werden. Diese Verfahren sind Eigenentwicklungen der DRV.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 16 von 40
--	---	-------------------------

- Rentenauszahlung (Schnittstelle)

Über das Verfahren „Rentenzahlverfahren“, das zentral bei der DSRV betrieben wird, wird der Auftrag zur Rentenauszahlung an den Rentenservice Deutsche Post AG (RS) als gesetzlich zuständige Stelle übermittelt. Die eigentliche Rentenauszahlung (Ausnahme knappschäftliche Inlandsrenten) erfolgt dann durch den RS.

- Bereitstellung der Liquidität

Damit der RS in der Lage ist, die monatlichen Renten auszuzahlen, muss diesem monatlich die finanziellen Mittel von den RVTR bereitgestellt werden. Die DRV Bund koordiniert im Rahmen ihrer Zuständigkeit als Grundsatz- und Querschnittsaufgabe diesen Prozess.

Die strukturierten Darstellungen zu diesen Prozessen sind der Anlage 2 zu entnehmen.

3.3 Branchenspezifische Gefährdungslage

3.3.1 All-Gefahrenansatz

Zur Betrachtung der Gefährdungslage ist die Behandlung aller relevanten Bedrohungen und Schwachstellen (All-Gefahrenansatz) für die den kDL zugrundeliegenden Verfahren und Infrastrukturen zwingende Voraussetzung.

Relevant für die kDL sind alle Bedrohungskategorien aus Anhang A, Punkt A1 und alle Schwachstellenkategorien aus Anhang A, Punkt A2. Diese entsprechen den in der Orientierungshilfe zum B3S aufgeführten und vom BSI im Rahmen des Lagebildes verwendeten Gefährdungskategorien.

3.3.2 Branchenspezifische Relevanz von Bedrohungen und Schwachstellen

Die Erbringung der kDL erfolgt auf Standard-IT-Systemen. Aus diesem Blickwinkel ist über die allgemeine Gefährdungslage hinaus keine besondere Gefährdungslage für branchenspezifische Systeme anzusetzen.

Eine branchenspezifische Gefährdungslage ergibt sich aus organisatorischer Sicht. Die weitreichende und tiefgreifende Abhängigkeit der organisatorischen Prozesse (gemeinsame Entwicklung und Pflege des Leistungssystems) und der technischen Anlagen sowie der bestehende Datenverkehr zwischen den RVTR stellt eine branchenspezifische Situation dar, aus der auch eine besondere Gefährdungslage hervorgeht.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 17 von 40
--	---	-------------------------

Am Rentenzahltag (letzter Werktag im Monat) müssen dem RS die notwendigen liquiden Mittel zur Verfügung stehen, um die Renten auszahlen zu können. Monatlich wird auf Grundlage der vom RS real zu zahlenden Rentenbeträge eine Liquiditätsbereitstellung zum Auszahlungstag erwartet. Da der RS diesbezüglich über keinen eigenen Finanzierungsrahmen oder Kreditmöglichkeiten verfügt, ist die Bereitstellung dieser Mittel wesentlich für eine ordnungsgemäße Rentenauszahlung.

Bei den von der DRV verarbeiteten Daten der Versicherten handelt es sich um Sozialdaten. Diese fallen somit unter das Sozialgeheimnis gem. § 35 Sozialgesetzbuch – 1. Buch (SGB I). Diese besagt, dass jeder einen Anspruch darauf hat, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden.

Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung auch innerhalb der einzelnen RVTR sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an solche weitergegeben werden. Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden.

3.3.3 Benennung der maßgeblichen Gefährdungen

Basierend auf den Auswirkungen für die kDL sind die nachfolgend aufgeführten Gefährdungen als maßgeblich anzusehen:

- Verlust der Integrität und Authentizität der Stammsatzdatei und Versicherungskonten,
- Ausfall des Verfahrens „eBanking“ am Auszahltag,
- Ausfall der Kommunikationsmittel Fax und Telefon am Auszahltag,
- Ausfall der Verfahren „rvDialog“, „rvPuR“ und „rvArchiv“,
- Ausfall des „DEÜV“ Verfahrens,
- Ausfall der DSRV,
- Ausfall der Basis-IT-Infrastruktur(en),
- Ausfall des DRV WAN (Verbindungsnetz der DRV).

Zu diesen Punkten müssen individuelle Betrachtungen der maßgeblichen Gefährdungen in den jeweiligen Basis- und verfahrensspezifischen IT-Sicherheitskonzepten der DRV erfolgen.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 18 von 40
--	---	-------------------------

3.4 Risikomanagement

3.4.1 Geeignete Behandlung aller für die kDL relevanten Risiken

Zur Identifizierung und Behandlung der relevanten Risiken sind für alle die kDL betreffenden Verfahren und deren zugrundeliegenden IT-Infrastrukturen Risikoanalysen zu erstellen.

Aufgrund der technischen und verfahrensbezogenen Vernetzung und Zusammenarbeit in der DRV ist eine DRV-weit einheitliche Vorgehensweise bei der Risikoanalyse unabdingbar, um eine einheitliche und vergleichbare Abschätzung der Risiken zu gewährleisten.

Dementsprechend müssen sowohl die in den Rechenzentren betriebenen Infrastrukturen als auch die kDL-relevanten Verfahren gemäß den übergreifend geltenden Vorgaben des Risikomanagements (siehe Kap. 4.4) in den Risikoanalysen als Bestandteil der jeweiligen Sicherheitskonzepte betrachtet werden. Die Risiken müssen mit Sicherheitsmaßnahmen belegt werden, die geeignet sind, diese angemessen zu reduzieren, um die Kontinuität der kDL sicherzustellen.

Die technischen und organisatorischen Vorkehrungen für die kDL müssen das Ziel verfolgen, Risiken zu vermeiden, insbesondere Risiken, welche die Versorgungsziele (Kritis-Schutzziele) gefährden.

Von wesentlicher Bedeutung ist dazu ein Risikomanagement, das die Risiken identifiziert, bewertet und deren Behandlung regelt. Dieses Risikomanagement ist in der Richtlinie „IT-Sicherheitskonzepte und Risikobehandlung“ beschrieben und muss im Sinne eines PDCA-Zyklus (Plan, Do, Check, Act) etabliert sein.

3.4.2 Beschränkung der Behandlungsalternativen für Risiken

Alle für die Erbringung der kDL maßgeblichen Risiken sind durch angemessene Maßnahmen abzuschern. Ist eine vollständige Absicherung nicht möglich, so sind die verbleibenden Risiken soweit möglich hinreichend zu reduzieren. Es ist dabei zu beachten, dass für die kDL-relevanten Risiken

- eine dauerhafte Risikoakzeptanz nicht möglich ist und
- diese auch nicht durch Versicherungen abgedeckt werden können, da hierdurch zwar der wirtschaftliche Schaden verringert werden könnte, die Auswirkungen in Bezug auf die kDL aber unverändert blieben.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 19 von 40
--	---	-------------------------

3.4.3 Berücksichtigung von Abhängigkeiten bei der Risikoanalyse

Da die IT-Systeme vollständig durch die DRV selbst sowie die eigenen IT-Dienstleister der DRV (Gesellschafter der IT-Dienstleister sind ausschließlich RVTR der DRV) betrieben werden, existieren keine Abhängigkeiten zu IT-Systemen Dritter.

Innerhalb der DRV sind übergreifend die Zuständigkeiten aller relevanten dezentralen und zentralen Verfahren, IT-Systeme und Infrastrukturen festzulegen, um eine vollständige Bewertung im Rahmen der Risikoanalysen zu gewährleisten.

Es muss dabei sichergestellt werden, dass die verfahrensspezifischen Risikoanalysen der RVTR sowohl auf die Risikoanalysen der relevanten Infrastrukturen als auch auf die Risikoanalysen der zentralen Verfahren (z.B. rvDialog) referenzieren.

Die externen Anbieter von Dienstleistungen sowie der externe Betreiber des DRV-WAN müssen die Mindestanforderungen der DRV über vertragliche Regelungen erfüllen.

3.4.4 Berücksichtigung der allgemeinen Gefährdungslage

Die allgemeine Gefährdungslage für die kDL-relevanten Systeme muss laufend überprüft werden. Dazu sind u.a. die Hinweise des BSI auf aktuelle Gefahrenlagen und weitere verfügbare Warnungen zu beachten.

Dabei müssen insbesondere berücksichtigt werden:

- allgemeine Bedrohungen und geänderte Gefährdungslage, z.B.
 - neu hinzugekommene Typen von Angreifern und Angriffen,
 - intensivere Aktivität oder verbesserte Expertise / Ressourcen von Angreifern,
 - Neuausrichtung von Angreifern,
- bekannt gewordene neue Schwachstellen,
- Änderungen der Gefährdungslage durch Veränderungen an der Systemarchitektur.

Die Berücksichtigung der allgemeinen Gefährdungslage erfolgt aufgrund der technischen und verfahrensbezogenen Vernetzung und Zusammenarbeit in der DRV federführend durch das CERT-DRV (Computer Emergency Response Team), welches die relevanten Informationen intern weitergibt und die internen Prozesse koordiniert.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 20 von 40
--	---	-------------------------

3.4.5 Berücksichtigung der branchenspezifischen Gefährdungslage

Die unter Kapitel 3.3 beschriebene branchenspezifische Gefährdungslage wird in der Betrachtung der DRV als kritische Infrastruktur berücksichtigt. Dies wird durch folgende Maßnahmen sichergestellt:

- Steuerung der DRV-übergreifenden IT-Sicherheit durch ein übergreifendes IT-Sicherheitsmanagement.
- Benennung eines gemeinsamen IT-Sicherheitsbeauftragten der DRV zur Koordinierung der RVTR.
- Betreiben einer Geschäftsstelle IT-Sicherheit für die RVTR-übergreifende Koordination und Abstimmung.
- Etablierung eines übergreifenden Gremiums zur IT-Sicherheit, das gemeinsame Entscheidungen zur IT-Sicherheit vorbereitet (Arbeitsgruppe Informationssicherheit [AGIS]).
- Verabschiedung einer DRV-weiten und verbindlichen Informationssicherheits-Policy als verbindliche Entscheidung des Bundesvorstands.
- Nutzung eines DRV-übergreifenden Systems zur Erstellung und Pflege von IT-Sicherheitskonzepten (einheitliche Konzeption und gemeinsames, zentrales ISM-Tool)
- Gewährleistung einer übergreifenden und gemeinsamen operativen IT-Sicherheit durch den Betrieb
 - eines übergreifenden CERT-DRV als Krisen- und Lagezentrum sowie koordinierende Instanz bei DRV-weiten Sicherheitsvorfällen und GÜAS-Funktionen als auch
 - der Security Operation Center in den Rechenzentrumsverbänden der DRV, die mit dem CERT-DRV zusammenarbeiten und systemnah für die operative IT-Sicherheit zuständig sind (Sicherheitsmonitoring, Behandlung von Sicherheitsvorfällen).

3.5 Fortschreibung des B3S

Dieser B3S beschreibt die Rahmenbedingungen und Anforderungen aus Sicht der Erstumsetzung der Anforderungen nach § 8a (3) BStG. Basierend auf den Erfahrungen der Anwender aus der Umsetzung und aus dem laufenden Betrieb muss der B3S durch die Geschäftsstelle für IT-Sicherheit (GSIS) der DRV fortgeschrieben werden.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 21 von 40
--------------------------------	---	------------------

4 Teil 2: Sicherheitsanforderungen nach Stand der Technik und Vorgehensweisen

4.1 Informationssicherheitsmanagementsystem (ISMS)

Ein ISMS nach IT-Grundschutz ist in der DRV zur nachhaltigen und angemessenen Planung, Steuerung, Kontrolle und Verbesserung der Informationssicherheit unabdingbar. Als wesentliche Bestandteile sind insbesondere der Aufbau einer Sicherheitsorganisation sowie die IT-Sicherheitskonzeption der DRV anzusehen.



Abbildung 2 Sicherheitskonzeption

Aufgrund der heterogenen Struktur und Arbeitsteilung der DRV und zur Sicherstellung einer DRV-weit einheitlichen Umsetzung müssen grundsätzliche Vorgaben zu den Prozessen und zur Organisation der Informationssicherheit übergreifend für alle RVTR, die DSRV sowie IT-Dienstleister der DRV verbindlich festgelegt werden. Die DRV hat dazu eine Sicherheitskonzeption entwickelt und mit der DRV-weit verbindlichen Informationssicherheits-Policy (ISP) einen Rahmen und ein Regelwerk erstellt, in dem die Vorgaben hierarchisch über fünf Ebenen festgelegt sind:

- Ebene 1: Leitlinie zur Informationssicherheit:
Die Leitlinie beschreibt die Sicherheitsstrategie sowie allgemeine Zielfestlegungen, welche

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 22 von 40
--	---	-------------------------

durch eine verbindliche Entscheidung des Bundesvorstandes der DRV Bund in Kraft gesetzt sind.

- Ebene 2: Grundzüge der Informationssicherheit (GdIS):
Die GdIS beschreibt unter anderem grundlegende Festlegungen für die Dokumente der ISP, langlebige Sicherheitsziele und -grundsätze für die DRV, die Umsetzung der Informationssicherheitsstrategie, Rahmenbedingungen und Aufgaben der IT-Sicherheitsbeauftragten (ITSIBE) sowie der Informations-Sicherheitsmanagement-Teams (ISMT) zur Unterstützung der ITSIBE.
- Die GdIS ist ebenfalls durch eine verbindliche Entscheidung des Bundesvorstandes der DRV Bund in Kraft gesetzt. Die in der GdIS beschriebenen Maßgaben und Zielsetzungen gelten unmittelbar und uneingeschränkt für alle Formen der Datenverarbeitung. Sie sind für alle RVTR und deren Beschäftigten verbindlich.
- Ebene 3: Richtlinien zu Teilbereichen der Informationssicherheit:
In den Richtlinien werden die in der GdIS vorgegebenen Sicherheitsanforderungen für abgegrenzte Themengebiete konkretisiert. Es wird unterschieden zwischen
 - für die gesamte DRV verbindliche Richtlinien und
 - regional- bzw. trägerspezifische Richtlinien.
- Anmerkung: Im Rahmen der Erstellung und Überarbeitung einer Richtlinie kann diese auch vorübergehend durch ein Dokument „AGIS-Mindestanforderungen“ für den entsprechenden Themenbereich ersetzt werden.
- Ebene 4: Konzepte zu Teilbereichen der Informationssicherheit:
In den Konzepten wird themenspezifisch dargestellt und festgelegt,
 - welche Daten in welcher Art und Weise und von welchen Stellen zu erheben und zu verarbeiten sind,
 - welche Rechtsgrundlagen dabei einzuhalten sind,
 - welche Technologien zum Einsatz kommen sollen und
 - welche Richtlinien dabei zu berücksichtigen sind.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 23 von 40
--	---	-------------------------

- Analog zu Ebene 3 wird auch auf Ebene 4 unterschieden zwischen
 - für die gesamte DRV verbindlichen Konzepten und
 - regional- bzw. trägerspezifischen Konzepten.
- Ebene 5: Handlungsanweisungen:
Die Handlungsanweisungen beschreiben konkret und zielgruppengerecht den Umgang mit IT-Systemen, IT-Verfahren, IT-Services etc.

Die Regelungen der GdIS und der für verbindlich erklärten Richtlinien zur Informationssicherheit bilden die Mindeststandards für die gesamte DRV, deren Sicherheitsniveau nicht unterschritten werden darf.

In der Richtlinie „Organisation der Informationssicherheit“ sind alle Richtlinien, Konzepte und Handlungsanweisungen aufgeführt, die DRV-weit verbindlich sind.

4.2 Erstellung von IT-Sicherheitskonzepten

4.2.1 Basis-IT-Sicherheitskonzepte

In der GdIS, Kap 4.3.2 sind wesentliche Standards geregelt. In der Sicherheitskonzeption der DRV wird der Umfang der Basis-IT-Sicherheitskonzepte geregelt. Für jede organisatorisch eigenständige Institution der DRV ist jeweils ein Basis-IT-Sicherheitskonzept zu erstellen. Ein weiteres Basis-IT-Sicherheitskonzept thematisiert das WAN der DRV.

Ziel ist es, einen angemessenen Schutz für alle Informationen einer Institution nach IT-Grundschutz zu erreichen.

Alle physischen Objekte sind im Basis-IT-Sicherheitskonzept zu betrachten.

4.2.2 IT-Verfahrenssicherheitskonzepte

Für alle IT-Verfahren hat der jeweilige Verfahrensverantwortliche auf Grundlage des Verfahrenszwecks in einem IT-Verfahrenssicherheitskonzept darzustellen, welche technischen und organisatorischen Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten getroffen wurden, um die Anforderungen des Verfahrens an die Informationssicherheit auf Grundlage der IT-Grundschutzkataloge zu erfüllen.

IT-Verfahrenssicherheitskonzepte setzen auf den Basis-IT-Sicherheitskonzepten auf.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 24 von 40
--	---	-------------------------

4.3 Asset Management

Die Assets der für die kDL maßgeblichen Verfahren inkl. der zugrundeliegenden Infrastruktur sind zur Identifikation, Klassifizierung und Inventarisierung zu dokumentieren. Die Dokumentation ist aktuell zu halten.

Grundlegende Anforderungen an das Asset Management sind übergreifend in der Richtlinie „IT-Systeme“ festgelegt und müssen DRV-weit einheitlich umgesetzt werden.

4.4 Risikoanalysemethoden

Zur Identifizierung und Behandlung der relevanten Risiken sind für alle die kDL betreffenden Verfahren sowie deren zugrundeliegenden IT-Infrastruktur und IT-Sicherheitskonzepte inkl. Risikoanalysen in Anlehnung an IT-Grundschutz zu erstellen.

Die Vorgehensweise zur Erstellung der Basis- und verfahrensspezifischen IT-Sicherheitskonzepte unter Berücksichtigung der gegenseitigen Abhängigkeiten im Rahmen der Risikoanalysen ist in der Richtlinie „IT-Sicherheitskonzepte und Risikobehandlung“ festgelegt und muss DRV-weit einheitlich umgesetzt werden.

Die Standards zur Schutzbedarfsfeststellung sind in der Richtlinie „Schutzziele und Schutzbedarf“ festgelegt und müssen DRV-weit einheitlich berücksichtigt werden.

4.5 Business Continuity Management (BCM) für kritische Dienstleistungen

Um sicherzustellen, dass die kDL selbst in kritischen Situationen und Notfällen nicht oder nur temporär unterbrochen werden und die Handlungsfähigkeit der DRV auch bei einem größeren Schadensereignis nicht längerfristig gefährdet wird, ist ein angemessenes Notfallmanagement (Business Continuity Management) in Anlehnung an die Standards des BSI erforderlich, welches sowohl die Notfallvorsorge als auch die Bewältigung eines Notfalls (Krisenmanagement) umfasst.

Von zentraler Bedeutung dabei ist ein auf den Risikoanalysen aufbauendes IT-Notfallvorsorgekonzept, in dem die Notfallvorsorgemaßnahmen festgelegt werden. Das IT-Notfallvorsorgekonzept ist regelmäßig zu prüfen und ggf. zu aktualisieren bzw. an den Stand der Technik anzupassen.

Ein funktionierendes Krisenmanagement erfordert die Festlegung einer Notfallorganisation, welche zusammen mit den Notfall- und Geschäftsfortführungsplänen im Notfallhandbuch zu dokumentieren sind.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 25 von 40
--	---	-------------------------

Die Wirksamkeit der Notfallmaßnahmen ist in regelmäßigen Abständen zu überprüfen (zum Beispiel durch Notfallübungen). Auf Basis der Erkenntnisse ist das Notfallmanagement zu optimieren.

Grundlegende Anforderungen an das Notfallmanagement sind übergreifend in der Richtlinie „Notfallvorsorge“ festgelegt und müssen DRV-weit umgesetzt werden. Zur Gewährleistung der Verfügbarkeit und Wiederherstellbarkeit der Daten nach einem Notfall sind die in der übergreifend gültigen Richtlinie „Datensicherung“ gemachten Vorgaben DRV-weit zu berücksichtigen.

4.6 Resiliente Architektur

Die Architektur der für den Betrieb der kDL erforderlichen IT-Systeme muss resilient sein, es müssen mindestens folgende Anforderungen (vgl. auch BCM, Kap. 4.5) berücksichtigt und umgesetzt werden:

- Aufstellung aller kDL-relevanten Systeme in ausreichend gesicherten Räumlichkeiten der DRV,
- Dedizierte Nutzung der zentralen kDL-relevanten Systeme für die kDL-relevanten Verfahren,
- Redundante Auslegung der IT-Systeme und Infrastrukturen, mit jeweils mindestens einer GEO-redundanten Auslagerung der Daten.

4.7 Branchenspezifische Technik

Bei den für den Betrieb der kDL eingesetzten Systemen handelt es sich um Standard-IT-Systeme, es kommt keine branchenspezifische Hardware zum Einsatz.

4.8 Technische Informationssicherheit

Für die Absicherung der kritischen Infrastruktur ist die technische Informationssicherheit von grundlegender Bedeutung. Maßgeblich für Regelungen und Maßnahmen zur Informationssicherheit sind die Standards des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dies ist in der Leitlinie zur Informationssicherheit festgelegt, die durch eine verbindliche Entscheidung des Bundesvorstands der DRV Bund für alle RVTR bindend ist.

In der GdIS und ausführlich in der DRV-weiten Richtlinie „IT-Sicherheitskonzepte und Risikobehandlung“ sind das Vorgehen und die Inhalte von Basis-IT-Sicherheitskonzepten (BSIKO) und von IT-Verfahrenssicherheitskonzepten geregelt sowie das Vorgehen zur Risikobehandlung.

Prüfgrundlage für den Nachweis sind die im Anhang 6.3 aufgeführten Richtlinien. Der Nachweis wird über die jeweiligen BSIKOs und die relevanten VSIKOs erbracht.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 26 von 40
--	---	-------------------------

Im Rahmen der Risikoanalyse sind alle für die kritische Infrastruktur auf Basis der im Anhang A aufgeführten Bedrohungs- und Schwachstellenkategorien identifizierten und relevanten Risiken zu berücksichtigen.

4.9 Personelle und organisatorische Sicherheit

Zur Vermeidung von Schäden an den kDL-relevanten Systemen oder bewusster oder unbewusster Manipulation der Daten sind geeignete personelle und organisatorische Maßnahmen zu treffen, die mindestens folgende Aspekte berücksichtigen:

- Sicherstellung der Fachkunde durch den Einsatz von geschultem Personal.
- Sicherstellung der Zuverlässigkeit durch geeignete Mechanismen (wo erforderlich z.B. durch Sicherheitsüberprüfungen oder Vorlage von Führungszeugnissen).
- Schaffung der Awareness für IT-Sicherheit auf allen Ebenen.
- Definition aller notwendigen Vorgaben für die Beschäftigten inkl. der Sanktionen bei Nichtbeachtung.
- Umsetzung eines Rollenkonzepts inkl. Ausschlussmatrix und Festlegung des Zwei-Personen-Prinzips, wo erforderlich.
- Umsetzung eines Identitäts- und Berechtigungsmanagements.
- Festlegung notwendiger Kompetenzen und Verantwortlichkeiten.
- Sicherstellung ausreichender Personalressourcen.

4.10 Bauliche und physische Sicherheit

Zur Vermeidung von Schäden an den zentralen kDL-relevanten Systemen durch Naturgefahren, Manipulation, Diebstahl, Zerstörung oder infrastrukturelle Mängel sind angemessene bauliche und physische Sicherheitsmaßnahmen in den Rechenzentren zu treffen, die folgende Aspekte (vgl. auch BCM, Kap. 4.5) berücksichtigen:

- Umfeldrisikoanalyse: Bewertung der Gefährdungspotentiale in der Umgebung.
- Bauliche Gegebenheiten: Bauliche Sicherheit bezüglich Fenstern, Türen, Brandabschnitten, Trassenverläufen.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 27 von 40
--	---	-------------------------

- Brandmelde- und Löschtechnik: Brandmeldeanlage mit Aufschaltung auf die Feuerwehr, Etablierung von Abschaltfunktionen und Schadensbegrenzungsmaßnahmen.
- Sicherheitssysteme: Zutrittskontrollanlagen, Videoüberwachung, Einbruchmeldeanlagen inkl. Aufschaltung auf ständig besetzte Sicherheitszentrale oder Polizei.
- Energieversorgung: Nach einschlägigen Normen erbrachte Installationen mit Überspannungsschutz und entsprechender unterbrechungsfreier Notstromversorgung.
- Raumluftechnische Anlagen: Klimatisierung der IT-Systeme und der Infrastrukturkomponenten.
- Organisation: Sicherstellung der regelmäßigen Prüfung und Wartung der Sicherheitseinrichtungen durch entsprechende Pläne und Verträge.

Die bauliche und physische Sicherheit ist in den Basis-IT-Sicherheitskonzepten der RVTR und der IT-Dienstleister zu betrachten. Des Weiteren sind in der übergreifend verbindlichen Richtlinie „Zutrittschutz“ grundlegende Vorgaben und Maßnahmen zur Gebäudehärtung und zu den erlaubten Methoden zur Zutrittssicherung aufgeführt, die DRV-weit berücksichtigt werden müssen.

4.11 Vorfallserkennung und –bearbeitung

Zur Erkennung und Bearbeitung von Vorfällen an den kDL-relevanten Systemen sind geeignete Maßnahmen zu treffen.

Vorfälle können sowohl Störungen sein, welche z.B. durch systematische Log-Auswertungen erkannt werden können, als auch Angriffe, welche z.B. durch Intrusion Detection Systeme (IDS) oder ein Security Information and Event Management System (SIEM) erkannt werden können.

Die zur Erkennung und Bearbeitung erforderlichen Tools und Prozesse sind durch fachkundiges Personal der operativen IT-Sicherheit zu betreiben. Bei den Betreibern der Rechenzentren der DRV sind dafür eigständige Bereiche (Security Operation Center, SOC) zu betreiben, die jeweils vom Bereich des IT-Betriebs unabhängig sind.

Das CERT-DRV übernimmt die Funktion einer „Gemeinsamen übergeordnete Ansprechstelle“ (GÜAS) gegenüber dem BSI (§8b BSIG) und koordiniert das Vorgehen bei DRV-weiten Sicherheitsvorfällen.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 28 von 40
--	---	-------------------------

In der übergreifend verbindlichen Richtlinie „Behandlung von Sicherheitsvorfällen“ sind Grundsatzvorgaben zu Meldewegen, Reaktionsprozessen und der Nachbereitung von Sicherheitsvorfällen aufgeführt, die DRV-weit berücksichtigt werden müssen.

4.12 Überprüfung

Um die Funktionsfähigkeit der eingesetzten Sicherungsmaßnahmen zu überprüfen und Schwachstellen zu identifizieren, sind regelmäßige (mind. alle zwei Jahre) Überprüfungen durchzuführen. Darüber hinaus müssen anlassbezogene Prüfungen durchgeführt werden, z. B. aufgrund von

- Änderungen in der Bedrohungs- oder Gefährdungslage,
- Änderungen an den IT- oder Kommunikationssystemen,
- nicht zuverlässig erklärbaren Beeinträchtigungen der KDL oder der zugehörigen IT-Systeme,
- erfolgreichen oder möglicherweise erfolgreichen Angriffen

Sowohl bei den regelmäßigen als auch anlassbezogenen Überprüfungen muss sichergestellt sein, dass alle Bereiche berücksichtigt werden:

- interne Überprüfungen bei den Institutionen der DRV müssen die jeweiligen IT-Sicherheitsbeauftragten koordinieren,
- übergreifende Überprüfungen zentraler bzw. trägerübergreifender Verfahren, Services und Dienste müssen durch den/die IT-Sicherheitsbeauftragte(n) der DRV und den ihm/ihr zugeordneten Organisationseinheiten koordiniert werden.

4.13 Externe Informationsversorgung und Unterstützung

Zur Aufrechterhaltung und stetigen Verbesserung des Sicherheitsniveaus sind regelmäßig und anlassbezogen Informationen über aktuelle Entwicklungen der IT-Sicherheitslage zu beschaffen. Neben den einschlägigen Informationsquellen im Internet ist insbesondere das BSI als Betreiber des CERT-Bund und der zentralen Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen nach §§ 8a bis 8c BSIG als Informationsquelle und zur Unterstützung einzubeziehen.

Die externe Informationsversorgung wird DRV-weit durch das CERT-DRV koordiniert, welches die relevanten Informationen intern an die beteiligten Rechenzentren, SOCs und RVTR weitergibt.

In der übergreifend verbindlichen Richtlinie „Behandlung von Sicherheitsvorfällen“ sind die Anforderungen an das CERT-DRV aufgeführt, die DRV-weit berücksichtigt werden müssen.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 29 von 40
--	---	-------------------------

4.14 Externe Dienstleister

Wie in Kap. 3.1.3 beschrieben, gelten für externe Dienstleister, welche relevante Anteile an der Erbringung der kDL haben, die gleichen Anforderungen an die IT-Sicherheit, wie für die DRV als Betreiber der kritischen Infrastruktur selbst.

Das Sicherheitsniveau der DRV darf durch externe Dienstleister nicht verschlechtert oder gefährdet werden. Ferner ist die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der zu verarbeitenden Daten entsprechend dem hohen Schutzbedarf sicherzustellen.

Um sicherzustellen, dass externe Dienstleister diese Anforderungen erfüllen, sind zum einen entsprechende Anforderungen in die Verträge aufzunehmen und zum anderen geeignete Nachweise zur Einhaltung der Anforderungen einzufordern (z.B. Herstellererklärungen, Zertifizierungen etc.) oder durch Auditierungen durch die DRV selbst oder unabhängige Dritte regelmäßig zu prüfen.

In der übergreifend verbindlichen Richtlinie „Aufgabenerledigung d. Dritte/Fernwartung“ sind die allgemeinen Vorgaben zur Einbindung externer Dienstleister aufgeführt, die DRV-weit berücksichtigt werden müssen.

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 30 von 40
--	---	-------------------------

5 Teil 3: Nachweisbarkeit der Umsetzung (Prüfungen)

§ 8a (3) BSIG schreibt den Betreibern Kritischer Infrastrukturen vor, mindestens alle zwei Jahre die Erfüllung der Anforderungen nach § 8a (1) BSIG auf geeignete Weise nachzuweisen. Für die DRV erfolgt der Nachweis gemäß Abstimmung durch ein zentrales Audit für alle RVTR.

Das zentrale Audit muss von erfahrenen Auditoren durchgeführt werden, welche neben ihren langjährigen IT-Sicherheits- und Auditkompetenzen sowohl die Prüfverfahrenskompetenz für § 8a (3) BSIG als auch hinreichende Branchenkompetenz nachweisen können.

Das zentrale Audit setzt sich aus zwei Komponenten zusammen:

- stichprobenartige Dokumentenprüfung der relevanten Informationssicherheitsdokumente und
- stichprobenartige Vor-Ort-Prüfungen.

Die Dokumentenprüfung ist „top down“ gemäß der in Kap. 4.1 aufgeführten hierarchischen Strukturen von den übergreifend geltenden Dokumenten (Leitlinie, GdIS, Richtlinien und Konzepte) zu den konkreten Sicherheitskonzepten der kDL-relevanten Verfahren und der zugrundeliegenden Infrastrukturen vorzunehmen.

In den Vor-Ort-Prüfungen müssen an zentraler Stelle die Umsetzung der in den Dokumenten beschriebenen Prozesse und Vorgaben geprüft werden. Darüber hinaus muss in mindestens einem repräsentativen Rechenzentrum die Umsetzung der baulichen und physischen Maßnahmen stichprobenartig geprüft werden.

Die Maßnahmen zur Informationssicherheit sind in folgenden BSIKOs behandelt. Alle physischen Objekte sind im Basis-IT-Sicherheitskonzept zu betrachten. Ferner sind grundsätzlich alle Bausteine aus dem IT-Grundschutz zu betrachten:

- BSIKO DRV WAN
- BSIKOs der IT-Dienstleister
- BSIKOs der RV-Träger
- BSIKO der DSRV

5.1 Kurzprüfungen

Zur Durchführung der Kurzprüfungen wurden anhand der Eigenheiten bei der Leistungserfüllung folgende Kategorien festgelegt:

Kategorie	Leistungserfüllung	Institution der DRV
K1	Eigenbetrieb	DRV Bund Träger DRV Knappschaft-Bahn-See DRV Berlin-Brandenburg
K2	Einkauf IT-Dienstleister	DRV Braunschweig-Hannover DRV Mitteldeutschland DRV Nord DRV Rheinland DRV Westfalen
K3	Nur Einkauf RZ	DRV Baden-Württemberg DRV Bayern Süd DRV Hessen DRV Nordbayern DRV Rheinland-Pfalz DRV Saarland DRV Schwaben
K4	RZ-Betrieb	DRV RZW GmbH
K5	IT-Dienstleister	DRV NOW-IT
K6	Gemischter Betrieb	DRV Bund GB0500 DRV Oldenburg-Bremen

Tabelle 2 Kurzprüfungen

Im Rahmen der Kurzprüfungen muss aus jeder Kategorie je mindestens eine Institution geprüft werden.

5.2 Querschnittsprüfungen

Im Rahmen der Querschnittsprüfungen wird sowohl die zentrale Implementierung als auch die Umsetzung einer Hausversion in mindestens einer Institution bzgl. der Umsetzung des Sicherheitskonzepts für die KRITIS-relevante Fachanwendung rvDialog im Detail geprüft:

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 32 von 40
------------------------------------	---	-------------------------

Audit	Auswahlkriterium	Auswahl
Q1	Wichtigkeit	rvDialog – zentrale Referenzversion
Q2	Wichtigkeit	rvDialog Hausversion

Tabelle 3 Querschnittsprüfung

5.3 Partialprüfungen

Die Partialprüfung beschränkt sich auf spezielle Ausschnitte (z.B. Geschäftsprozesse) und betrachtet diese im Detail. Aufgrund der Wichtigkeit für die Erbringung der kDL wurden folgende Prozesse für die Partialprüfung festgelegt, die jeweils bei mindestens einer Institution der DRV geprüft werden müssen:

Audit	Auswahl
P1	Incident-Handling
P2	Liquiditätsbereitstellungsprozess
P3	Knappschaftliches Auszahlungssystem

Tabelle 4 Partialprüfung

5.4 Einsichtnahme durch das BSI

Unabhängig von erkannten Sicherheitsmängeln kann das BSI die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen.

6 Anhang A: Maßnahmen zur Behandlung von Bedrohungen und Schwachstellen

6.1 Mögliche Bedrohungen

Hacking und Manipulation
Terroristische Akte (Physisch mit Wirkung auf die IT oder direkt IT-bezogen)
Naturgefahren mit Wirkung auf die IT
Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)
Missbrauch (Innentäter)
Abhängigkeiten von externen Dienstleistern und Herstellern (Ausfall für IT-Betrieb erforderlicher externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)
Unbefugter Zugriff
Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen
Schadprogramme
Social Engineering
Gezielte Störung/Verhinderung von Diensten (DdoS, gezielte Systemabstürze, ...)
Advanced Persistent Threat (APT)
Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systeme
Ausfall von Basisinfrastrukturen mit direktem Bezug zur IT (Sekundäreffekte, z. B. Strom und TK)

6.2 Mögliche Schwachstellen

Organisatorische Mängel
Technische Schwachstellen in Software, Firmware und Hardware
Technisches Versagen von IT-Systemen, IT-Verfahren oder Datennetzen (sowie Verlust von gespeicherten Daten)
Menschliche Fehlhandlungen, menschliches Versagen
Infrastrukturelle Mängel (baulich, Versorgung mit Strom etc.)
Verwendung ungeeigneter Netze/Kommunikationsverbindungen, sonstige Schwächen in der Kommunikationsarchitektur
Verkopplung von Diensten (Beeinträchtigung eines Dienstes durch Störung anderer Dienste)

6.3 Richtlinien und damit verbundene Maßnahmen zur Behandlung von Bedrohungen und Schwachstellen:

Die DRV hat im Rahmen ihrer Sicherheitskonzeption durch ihre DRV-weit verbindlichen Richtlinien Mindeststandards für alle Institutionen der DRV erlassen, die den o.g. Bedrohungen und Schwachstellen gerecht werden. Die Richtlinien und ihr grundsätzlicher Regelungsrahmen ist der folgenden Tabelle zu entnehmen.

Richtlinie	Regelung / Schwerpunkte
Organisation der Informationssicherheit	Globale Vorgaben für das ISMS der DRV, Organisation und Policy
Schutzziele und Schutzbedarf	U. a. Schutzbedarfsanalyse und -feststellung
Zutrittsschutz	Vorgaben/Maßnahmen zur Gebäudehärtung, Zutrittssicherung und Zutrittskontrolle.

Richtlinie	Regelung / Schwerpunkte
Zugangs- und Zugriffsschutz	Benutzerverwaltung, Rechte- und Rollenkonzepte, Protokollierungen
IT-Systeme	Grundsätzliche Absicherung von Server und Host, Geräte- und Anlagenverzeichnis, CMDB, Schutz vor Schadprogrammen etc.
Endgeräte	Grundsatzvorgaben für die Endgeräte, auch bei häuslichem oder mobilem Einsatz, Schutz vor Schadprogrammen
Datennetz	Ausführungen zum WAN und Grundsätze zum LAN der einzelnen Institutionen. Zentrales Gateway, Schutzmaßnahmen und Absicherung der Netzübergänge, IDS und IPS
Elektronischer Datenaustausch	Standards für Datenaustausch über zulässige Kommunikationswege, Sichere Interaktion im Internet (z. B. E-Mail, De-Mail, Dateianhänge, Messenger, Datenträger, DOI oder eXtra)
Telekommunikation	Videokonferenz, Videotelefonie, VOIP, klassische Telefonie
Datenlöschung	Grundsatzvorgaben zur Datenlöschung und -vernichtung elektronischer und nichtelektronischer Medien
Datensicherung	Grundsatzvorgaben zur Datensicherung, Redundanzen
Archivierung	Grundsatzvorgaben zur Datenarchivierung
Entwicklung und Anpassung von IT-Verfahren	Grundsatzvorgaben zur Softwareentwicklung. Test und Freigabeverfahren, Dokumentation, SuSy und EFA/KC Prinzipien
Betrieb IT-Verfahren und Anwendungen	Change- und Patchmanagement, Administrationskonzepte, Dokumentation, IT-Verfahrensverzeichnis etc.
Sicherheitskonzepte und Risikobehandlung	Sicherheitskonzeption der DRV, Basis-IT-Sicherheitskonzepte, IT-Verfahrenssicherheitskonzepte und Risikobehandlung
Kryptografische Verfahren und Produkte	Grundsätze zur Verschlüsselung und Kryptografie, Darstellung der Verschlüsselung auf verschiedenen Ebenen (OSI Schichtenmodell);
Identitätsmanagement und Berechtigungsmanagement	Grundsatzvorgaben zur sicheren Authentifizierung (Login), ePA, elektronische Signaturen, Unterschriftenpad, Trustcenter etc.
Sicherheitsvorfälle	Grundsatzvorgaben zu Meldewegen, Reaktionsprozesse, CERT/SOC, Nachbereitung von Sicherheitsvorfällen
Notfallvorsorge	Grundsatzvorgaben zur Notfallvorsorge und Krisenmanagement

7 Anhang B: Verzeichnisse

7.1 Abkürzungen

Begriff	Beschreibung
AG	Aktiengesellschaft
AGIS	Arbeitsgruppe Informationssicherheit
APT	Advanced Persistent Threat
B3S	Branchenspezifische Sicherheitsstandards
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSIKO	Basis-IT-Sicherheitskonzept
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BVA	Bundesversicherungsamt
BYOD	Bring your own device
CERT	Computer Emergency Response Team
DEÜV	Datenerfassungs- und -übermittlungsverordnung
DDoS	Distributed Denial of Service
DRV	Deutsche Rentenversicherung
DSRV	Datenstelle der Rentenversicherung
GB0500	Geschäftsbereich 0500 der DRV Bund
GdIS	Grundzüge der Informationssicherheit

Begriff	Beschreibung
GmbH	Gesellschaft mit beschränkter Haftung
GSIS	Geschäftsstelle für IT-Sicherheit
GÜAS	Gemeinsame übergreifende Ansprechstelle
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Informations-Sicherheits-Management System
ISMT	Informations-Sicherheits-Management Team
ISP	Informationssicherheits-Policy
IT	Informationstechnik
ITSIBE	IT-Sicherheitsbeauftragter
kDL	kritische Dienstleistung
KBS	Knappschaft-Bahn-See
KRITIS	Kritische Infrastruktur
NAC	Network Access Control
NOW IT GmbH	Nord Ost West Informationstechnik
RS	Rentenservice Deutsche Post AG
SGB	Sozialgesetzbuch
SIEM	Security Information and Event Management
SOC	Security Operation Centre

Begriff	Beschreibung
RVTR	Träger der Deutschen Rentenversicherung
RZ	Rechenzentrum
RZW GmbH	Rechenzentrum Würzburg
TK	Telekommunikation
USV	Unterbrechungsfreie Stromversorgung
VPN	Virtuelles privates Netzwerk
WAN	Wide Area Network

7.2 Abbildungen

Abbildung 1 Technische Anlagen	9
Abbildung 2 Sicherheitskonzeption.....	21

7.3 Tabellen

Tabelle 1: Schutzbedarf.....	14
Tabelle 2 Kurzprüfungen	31
Tabelle 3 Querschnittsprüfung.....	32
Tabelle 4 Partialprüfung.....	32
Tabelle 2 Kurzprüfungen	31
Tabelle 3 Querschnittsprüfung.....	32
Tabelle 4 Partialprüfung.....	32

7.4 Referenzierte Dokumente

Nr.	Dokument
1	BSI, KRITIS-Sektorstudie Finanz- und Versicherungswesen, 18.12.2015
2	Bundesregierung, Erste Verordnung zur Änderung der BSI-Kritisverordnung, 21.6.2017

Nr.	Dokument
3	Bundesregierung, Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), 22.4.2016
4	Bundesregierung, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 17.7.2015
5	Bundesregierung, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, 14.8.2009
6	BSI, Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG, 01.12.2017
7	Leitlinie zur Informationssicherheit
8	Grundzüge der Informationssicherheit (GdIS)
9	Richtlinie Organisation der Informationssicherheit
10	Richtlinie Schutzziele und Schutzbedarf
11	Richtlinie IT-Sicherheitskonzepte und Risikobehandlung
12	Richtlinie IT-Systeme
13	Richtlinie Notfallvorsorge
14	Richtlinie Datensicherung
15	Richtlinie Zutrittsschutz
16	Richtlinie Behandlung von Sicherheitsvorfällen
17	Richtlinie Aufgabenerledigung d. Dritte/Fernwartung

Abbildung 1 Technische Anlagen 9

Abbildung 2 Sicherheitskonzeption..... 21

Deutsche Rentenversicherung	Deutsche Rentenversicherung Branchenspezifischer Sicherheitsstandard	Seite: 40 von 40
--	---	-------------------------

7.5 Anlagen

Anlage 1 - Gesetzliche Grundlagen (Auszüge aus dem Gesetzestext)

Anlage 2 – Darstellung der kDL als vereinfachter Netzplan

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

SGB I § 12 Leistungsträger

Zuständig für die Sozialleistungen sind die in den §§ 18 bis 29 genannten Körperschaften, Anstalten und Behörden (Leistungsträger). Die Abgrenzung ihrer Zuständigkeit ergibt sich aus den besonderen Teilen dieses Gesetzbuchs.

SGB IV § 29 Rechtsstellung

- (1) Die Träger der Sozialversicherung (Versicherungsträger) sind rechtsfähige Körperschaften des öffentlichen Rechts mit Selbstverwaltung.
- (2) Die Selbstverwaltung wird, soweit § 44 nichts Abweichendes bestimmt, durch die Versicherten und die Arbeitgeber ausgeübt.
- (3) Die Versicherungsträger erfüllen im Rahmen des Gesetzes und des sonstigen für sie maßgebenden Rechts ihre Aufgaben in eigener Verantwortung.

SGB IV § 90 Aufsichtsbehörden

- (1) Die Aufsicht über die Versicherungsträger, deren Zuständigkeitsbereich sich über das Gebiet eines Landes hinaus erstreckt (bundesunmittelbare Versicherungsträger), führt das Bundesversicherungsamt, auf den Gebieten der Prävention in der gesetzlichen Unfallversicherung das Bundesministerium für Arbeit und Soziales. Die Aufsicht über die Unfallversicherung Bund und Bahn auf dem Gebiet der Prävention führt das Bundesministerium des Innern.
- (2) Die Aufsicht über die Versicherungsträger, deren Zuständigkeitsbereich sich nicht über das Gebiet eines Landes hinaus erstreckt (landesunmittelbare Versicherungsträger), führen die für die Sozialversicherung zuständigen obersten Verwaltungsbehörden der Länder oder die von den Landesregierungen durch Rechtsverordnung bestimmten Behörden; die Landesregierungen können diese Ermächtigung auf die obersten Landesbehörden weiter übertragen.
- (2a) Die Aufsicht über die Deutsche Rentenversicherung Bund führt das Bundesversicherungsamt. Soweit die Deutsche Rentenversicherung Bund Grundsatz- und Querschnittsaufgaben wahrnimmt, führt das Bundesministerium für Arbeit und Soziales die Aufsicht; es kann die Aufsicht teilweise dem Bundesversicherungsamt übertragen.
- (3) Abweichend von Absatz 1 führen die Verwaltungsbehörden nach Absatz 2 die Aufsicht über Versicherungsträger, deren Zuständigkeitsbereich sich über das Gebiet eines Landes, aber nicht über mehr als drei Länder hinaus erstreckt und für die das aufsichtführende Land durch die beteiligten Länder bestimmt ist.
- (4) Die Aufsichtsbehörden treffen sich regelmäßig zu einem Erfahrungsaustausch. Soweit dieser Erfahrungsaustausch Angelegenheiten der Sozialversicherung für Landwirtschaft, Forsten und Gartenbau betrifft, nehmen auch das Bundesministerium für Arbeit und Soziales und das Bundesministerium für Ernährung und Landwirtschaft teil.

SGB VI § 118 Fälligkeit und Auszahlung

- (1) Laufende Geldleistungen mit Ausnahme des Übergangsgeldes werden am Ende des Monats fällig, zu dessen Beginn die Anspruchsvoraussetzungen erfüllt sind; sie werden am letzten Bankarbeitstag dieses Monats ausgezahlt. Bei Zahlung auf ein Konto im Inland ist die Gutschrift der laufenden Geldleistung, auch wenn sie nachträglich erfolgt, so vorzunehmen, dass die Wertstellung des eingehenden Überweisungsbetrages auf dem Empfängerkonto

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

unter dem Datum des Tages erfolgt, an dem der Betrag dem Geldinstitut zur Verfügung gestellt worden ist. Für die rechtzeitige Auszahlung im Sinne von Satz 1 genügt es, wenn nach dem gewöhnlichen Verlauf die Wertstellung des Betrages der laufenden Geldleistung unter dem Datum des letzten Bankarbeitstages erfolgen kann.

(2) Laufende Geldleistungen, die bei Auszahlungen

1.

im Inland den aktuellen Rentenwert,

2.

im Ausland das Dreifache des aktuellen Rentenwerts nicht übersteigen,

können für einen angemessenen Zeitraum im Voraus ausgezahlt werden.

(2a) Nachzahlungsbeträge, die ein Zehntel des aktuellen Rentenwerts nicht übersteigen, sollen nicht ausgezahlt werden.

(3) Geldleistungen, die für die Zeit nach dem Tod des Berechtigten auf ein Konto bei einem Geldinstitut, für das die Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl. L 94 vom 30.3.2012, S. 22) gilt, überwiesen wurden, gelten als unter Vorbehalt erbracht. Das Geldinstitut hat sie der überweisenden Stelle oder dem Träger der Rentenversicherung zurückzuüberweisen, wenn diese sie als zu Unrecht erbracht zurückfordern. Eine Verpflichtung zur Rücküberweisung besteht nicht, soweit über den entsprechenden Betrag bei Eingang der Rückforderung bereits anderweitig verfügt wurde, es sei denn, dass die Rücküberweisung aus einem Guthaben erfolgen kann. Das Geldinstitut darf den überwiesenen Betrag nicht zur Befriedigung eigener Forderungen verwenden.

(4) Soweit Geldleistungen für die Zeit nach dem Tod des Berechtigten zu Unrecht erbracht worden sind, sind sowohl die Personen, die die Geldleistungen unmittelbar in Empfang genommen haben oder an die der entsprechende Betrag durch Dauerauftrag, Lastschrifteinzug oder sonstiges bankübliches Zahlungsgeschäft auf ein Konto weitergeleitet wurde (Empfänger), als auch die Personen, die als Verfügungsberechtigte über den entsprechenden Betrag ein bankübliches Zahlungsgeschäft zu Lasten des Kontos vorgenommen oder zugelassen haben (Verfügende), dem Träger der Rentenversicherung zur Erstattung des entsprechenden Betrages verpflichtet. Der Träger der Rentenversicherung hat Erstattungsansprüche durch Verwaltungsakt geltend zu machen. Ein Geldinstitut, das eine Rücküberweisung mit dem Hinweis abgelehnt hat, dass über den entsprechenden Betrag bereits anderweitig verfügt wurde, hat der überweisenden Stelle oder dem Träger der Rentenversicherung auf Verlangen Name und Anschrift des Empfängers oder Verfügenden und etwaiger neuer Kontoinhaber zu benennen. Ein Anspruch gegen die Erben nach § 50 des Zehnten Buches bleibt unberührt.

(4a) Die Ansprüche nach den Absätzen 3 und 4 verjähren in vier Jahren nach Ablauf des Kalenderjahres, in dem der Träger der Rentenversicherung Kenntnis von der Überzahlung und in den Fällen des Absatzes 4 zusätzlich Kenntnis von dem Erstattungspflichtigen erlangt hat. Für die Hemmung, die Ablaufhemmung, den Neubeginn und die Wirkung der Verjährung gelten die Vorschriften des Bürgerlichen Gesetzbuchs sinngemäß.

(5) Sind laufende Geldleistungen, die nach Absatz 1 auszusahlen und in dem Monat fällig geworden sind, in dem der Berechtigte verstorben ist, auf das bisherige Empfängerkonto bei einem Geldinstitut überwiesen worden, ist der Anspruch der Erben gegenüber dem Träger der Rentenversicherung erfüllt.

SGB VI

§ 119 Wahrnehmung von Aufgaben durch die Deutsche Post AG

(1) Die Träger der allgemeinen Rentenversicherung zahlen die laufenden Geldleistungen mit Ausnahme des Übergangsgeldes durch die Deutsche Post AG aus. Im Übrigen können die

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

Träger der Rentenversicherung Geldleistungen durch die Deutsche Post AG auszahlen lassen.

(2) Soweit die Deutsche Post AG laufende Geldleistungen für die Träger der Rentenversicherung auszahlt, führt sie auch Arbeiten zur Anpassung der Leistungen durch. Die Anpassungsmittelungen ergehen im Namen des Trägers der Rentenversicherung.

(3) Die Auszahlung und die Durchführung der Anpassung von Geldleistungen durch die Deutsche Post AG umfassen auch die Wahrnehmung der damit im Zusammenhang stehenden Aufgaben der Träger der Rentenversicherung, insbesondere

1. die Überwachung der Zahlungsvoraussetzungen durch die Auswertung der Sterbefallmitteilungen nach § 101a des Zehnten Buches und durch die Einholung von Lebensbescheinigungen im Rahmen des § 60 Abs. 1 und des § 65 Abs. 1 Nr. 3 des Ersten Buches sowie die Erstellung statistischen Materials und dessen Übermittlung an das
2. Bundesministerium für Arbeit und Soziales und an die Deutsche Rentenversicherung Bund.

(4) Die Träger der Rentenversicherung werden von ihrer Verantwortung gegenüber dem Leistungsberechtigten nicht entbunden. Der Leistungsberechtigte soll jedoch Änderungen in den tatsächlichen oder rechtlichen Verhältnissen, die für die Auszahlung oder die Durchführung der Anpassung der von der Deutschen Post AG gezahlten Geldleistungen erheblich sind, unmittelbar der Deutschen Post AG mitteilen.

(5) Zur Auszahlung der Geldleistungen erhält die Deutsche Post AG von den Trägern der Rentenversicherung monatlich rechtzeitig angemessene Vorschüsse. Die Deutsche Rentenversicherung Bund setzt für die Träger der allgemeinen Rentenversicherung die Vorschüsse fest.

(6) Die Deutsche Post AG erhält für ihre Tätigkeit von den Trägern der Rentenversicherung eine angemessene Vergütung und auf die Vergütung monatlich rechtzeitig angemessene Vorschüsse. Die Deutsche Rentenversicherung Bund setzt für die Träger der allgemeinen Rentenversicherung die Vorschüsse fest.

SGB VI

§ 138 Grundsatz- und Querschnittsaufgaben der Deutschen Rentenversicherung

(1) Die Deutsche Rentenversicherung Bund nimmt die Grundsatz- und Querschnittsaufgaben der Deutschen Rentenversicherung wahr. Dazu gehören:

1. Vertretung der Rentenversicherung in ihrer Gesamtheit gegenüber Politik, Bundes-, Landes-, Europäischen und sonstigen nationalen und internationalen Institutionen sowie Sozialpartnern, Abstimmung mit dem verfahrensführenden Träger der Rentenversicherung in Verfahren vor dem Europäischen Gerichtshof, dem Bundesverfassungsgericht und dem Bundessozialgericht,
2. Öffentlichkeitsarbeit einschließlich der Herausgabe von regelmäßigen Informationen zur Alterssicherung für Arbeitgeber, Versicherte und Rentner und der Grundsätze für regionale Broschüren,
3. Statistik,
- 4.

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

Klärung von grundsätzlichen Fach- und Rechtsfragen zur Sicherung der einheitlichen Rechtsanwendung aus den Bereichen

- a)
Rehabilitation und Teilhabe,
- b)
Sozialmedizin,
- c)
Versicherung,
- d)
Beitrag,
- e)
Beitragsüberwachung,
- f)
Rente,
- g)
Auslandsrecht, Sozialversicherungsabkommen, Recht der Europäischen Union, soweit es die Rentenversicherung betrifft,

5.
Organisation des Qualitäts- und Wirtschaftlichkeitswettbewerbs zwischen den Trägern, insbesondere Erlass von Rahmenrichtlinien für Aufbau und Durchführung eines zielorientierten Benchmarking der Leistungs- und Qualitätsdaten,
6.
Grundsätze für die Aufbau- und Ablauforganisation, das Personalwesen und Investitionen unter Wahrung der Selbständigkeit der Träger,
7.
Grundsätze und Steuerung der Finanzausstattung und -verwaltung im Rahmen der Finanzverfassung für das gesamte System,
8.
Koordination der Planung von Rehabilitationsmaßnahmen, insbesondere der Bettenbedarfs- und Belegungsplanung,
9.
Grundsätze und Koordination der Datenverarbeitung und Servicefunktionen,
10.
Funktion zur Registrierung und Authentifizierung für die elektronischen Serviceangebote der Rentenversicherung,
11.
Funktion als Signaturstelle,
12.
Grundsätze für die Aus- und Fortbildung,
13.
Grundsätze der Organisation und Aufgabenzuweisung der Auskunft- und Beratungsstellen,
14.
Bereitstellung von Informationen für die Träger der Rentenversicherung,
15.
Forschung im Bereich der Alterssicherung und der Rehabilitation und
- 16.

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

Treuhänderschaft gemäß dem Gesetz zur Regelung der Rechtsverhältnisse der unter Artikel 131 des Grundgesetzes fallenden Personen.

(2) Die Entscheidungen der Deutschen Rentenversicherung Bund zu Grundsatz- und Querschnittsaufgaben der Deutschen Rentenversicherung sowie die notwendig werdende Festlegung weiterer Grundsatz- und Querschnittsaufgaben werden durch die Bundesvertreterversammlung der Deutschen Rentenversicherung Bund gemäß § 64 Abs. 4 des Vierten Buches getroffen; für die Träger der Rentenversicherung sind die Entscheidungen verbindlich. Die Bundesvertreterversammlung kann die Entscheidungsbefugnis gemäß § 64 Abs. 4 des Vierten Buches ganz oder teilweise auf den Bundesvorstand der Deutschen Rentenversicherung Bund übertragen, der gemäß § 64 Abs. 4 des Vierten Buches entscheidet. Entscheidungen über die Auslegung von Rechtsfragen werden von der Bundesvertreterversammlung und vom Bundesvorstand mit der einfachen Mehrheit aller gewichteten Stimmen der satzungsmäßigen Mitgliederzahl getroffen.

(3) Der Bundesvorstand kann die Entscheidungsbefugnis gemäß § 64 Abs. 4 des Vierten Buches ganz oder teilweise auf einen Ausschuss des Bundesvorstandes übertragen. Die Entscheidungen dieses Ausschusses müssen einstimmig ergehen. Der Ausschuss legt dem Bundesvorstand die Entscheidungen vor; der Bundesvorstand kann gemäß § 64 Abs. 4 des Vierten Buches abweichende Entscheidungen treffen.

(4) Soweit das Direktorium Vorlagen an die Bundesvertreterversammlung oder den Bundesvorstand unterbreitet, die verbindliche Entscheidungen oder notwendig werdende Festlegungen weiterer Grundsatz- und Querschnittsaufgaben betreffen, bedürfen diese der vorherigen Zustimmung durch das Erweiterte Direktorium. Beratungsergebnisse der Fachausschüsse, in denen alle Träger der Rentenversicherung vertreten sind, sind an die Bundesvertreterversammlung oder den Bundesvorstand weiterzuleiten. Das Nähere regelt die Satzung.

(5) Die verbindlichen Entscheidungen und die Festlegung weiterer Grundsatz- und Querschnittsaufgaben werden im Amtlichen Mitteilungsblatt der Deutschen Rentenversicherung Bund veröffentlicht.

SGB VI

§ 145 Aufgaben der Datenstelle der Rentenversicherung

(1) Die Träger der Rentenversicherung unterhalten gemeinsam eine Datenstelle, die von der Deutschen Rentenversicherung Bund verwaltet wird. Dabei 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 Träger der Rentenversicherung können die Datenstelle als Vermittlungsstelle einschalten. Sie können durch die Datenstelle auch die Ausstellung von Sozialversicherungsausweisen veranlassen.

(2) Die Deutsche Rentenversicherung Bund darf eine Datei mit Sozialdaten, die nicht ausschließlich einer Versicherungsnummer der bei ihr Versicherten zugeordnet ist, nur bei der Datenstelle und nur dann führen, wenn die Einrichtung dieser Datei gesetzlich bestimmt ist.

(3) Die Deutsche Rentenversicherung Bund kann durch öffentlich-rechtlichen Vertrag die Verpflichtung eingehen, dass die Datenstelle in Versorgungsausgleichssachen die Aufgabe als Vermittlungsstelle zur Durchführung des elektronischen Rechtsverkehrs auch für andere öffentlich-rechtliche Versorgungsträger wahrnimmt. Diese sind verpflichtet, der Deutschen Rentenversicherung Bund den entstehenden Aufwand zu erstatten.

(4) Die Datenstelle untersteht der Aufsicht des Bundesministeriums für Arbeit und Soziales, soweit ihr durch Gesetz oder auf Grund eines Gesetzes Aufgaben zugewiesen worden sind. Für die Aufsicht gelten die §§ 87 bis 89 des Vierten Buches entsprechend. Das Bundesministerium für Arbeit und Soziales kann die Aufsicht ganz oder teilweise dem Bundesversicherungsamt übertragen.

(5) (weggefallen)

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

SGB VI § 149 Versicherungskonto

(1) Der Träger der Rentenversicherung führt für jeden Versicherten ein Versicherungskonto, das nach der Versicherungsnummer geordnet ist. In dem Versicherungskonto sind die Daten, die für die Durchführung der Versicherung sowie die Feststellung und Erbringung von Leistungen einschließlich der Rentenauskunft erforderlich sind, zu speichern. Ein Versicherungskonto darf auch für Personen geführt werden, die nicht nach den Vorschriften dieses Buches versichert sind, soweit es für die Feststellung der Versicherungs- oder Beitragspflicht und für Prüfungen bei Arbeitgebern (§ 28p des Vierten Buches) erforderlich ist.

(2) Der Träger der Rentenversicherung hat darauf hinzuwirken, dass die im Versicherungskonto gespeicherten Daten vollständig und geklärt sind. Die Daten sollen so gespeichert werden, dass sie jederzeit abgerufen und auf maschinell verwertbaren Datenträgern oder durch Datenübertragung übermittelt werden können. Stellt der Träger der Rentenversicherung fest, dass für einen Beschäftigten mehrere Beschäftigungen nach § 8 Abs. 1 Nr. 1 oder § 8a des Vierten Buches gemeldet oder die Zeitgrenzen des § 8 Abs. 1 Nr. 2 des Vierten Buches überschritten sind, überprüft er unverzüglich diese Beschäftigungsverhältnisse. Stellen die Träger der Rentenversicherung fest, dass eine Beschäftigung infolge einer Zusammenrechnung versicherungspflichtig ist, sie jedoch nicht oder als versicherungsfrei gemeldet worden ist, teilen sie diese Beschäftigung mit den notwendigen Daten der Einzugsstelle mit. Satz 4 gilt entsprechend, wenn die Träger der Rentenversicherung feststellen, dass beim Zusammentreffen mehrerer Beschäftigungsverhältnisse die Voraussetzungen für die Anwendung der Vorschriften über die Gleitzone nicht oder nicht mehr vorliegen.

(3) Der Träger der Rentenversicherung unterrichtet die Versicherten regelmäßig über die in ihrem Versicherungskonto gespeicherten Sozialdaten, die für die Feststellung der Höhe einer Rentenanwartschaft erheblich sind (Versicherungsverlauf).

(4) Versicherte sind verpflichtet, bei der Klärung des Versicherungskontos mitzuwirken, insbesondere den Versicherungsverlauf auf Richtigkeit und Vollständigkeit zu überprüfen, alle für die Kontenklärung erheblichen Tatsachen anzugeben und die notwendigen Urkunden und sonstigen Beweismittel beizubringen.

(5) Hat der Versicherungsträger das Versicherungskonto geklärt oder hat der Versicherte innerhalb von sechs Kalendermonaten nach Versendung des Versicherungsverlaufs seinem Inhalt nicht widersprochen, stellt der Versicherungsträger die im Versicherungsverlauf enthaltenen und nicht bereits festgestellten Daten, die länger als sechs Kalenderjahre zurückliegen, durch Bescheid fest. Bei Änderung der dem Feststellungsbescheid zugrunde liegenden Vorschriften ist der Feststellungsbescheid durch einen neuen Feststellungsbescheid oder im Rentenbescheid mit Wirkung für die Vergangenheit aufzuheben; die §§ 24 und 48 des Zehnten Buches sind nicht anzuwenden. Über die Anrechnung und Bewertung der im Versicherungsverlauf enthaltenen Daten wird erst bei Feststellung einer Leistung entschieden.

SGB VI § 151a Antragstellung im automatisierten Verfahren beim Versicherungsamt

(1) Für die Aufnahme von Leistungsanträgen bei dem Versicherungsamt oder der Gemeindebehörde und die Übermittlung der Anträge an den Träger der Rentenversicherung kann ein automatisiertes Verfahren eingerichtet werden, das es dem Versicherungsamt oder der Gemeindebehörde ermöglicht, die für das automatisierte Verfahren erforderlichen Daten der Versicherten, aus der Stammsatzdatei der Datenstelle der Rentenversicherung (§ 150 Abs. 2) und dem Versicherungskonto (§ 149 Abs. 1) abzurufen, wenn die Versicherten oder anderen Leistungsberechtigten ihren Wohnsitz oder gewöhnlichen Aufenthalt, ihren

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

Beschäftigungsort oder Tätigkeitsort im Bezirk des Versicherungsamtes oder in der Gemeinde haben.

(2) Aus der Stammsatzdatei dürfen nur die in § 150 Abs. 2 Nr. 1 bis 4 genannten Daten abgerufen werden. Aus dem Versicherungskonto dürfen nur folgende Daten und die Angabe des aktuell kontoführenden Rentenversicherungsträgers abgerufen werden:

1. Datum des letzten Zuzugs aus dem Ausland unter Angabe des Staates,
2. Datum der letzten Kontoklärung,
3. Anschrift,
4. Datum des Eintritts in die Versicherung,
5. Lücken im Versicherungsverlauf, an deren Klärung der Versicherte noch nicht mitgewirkt hat,
6. Kindererziehungszeiten und Berücksichtigungszeiten,
7. Berufsausbildungszeiten,
8. Wartezeitauskunft zu der beantragten Rente einschließlich der Wartezeiterfüllung nach § 52,
- 9.

die zuständigen Einzugsstellen mit Angabe des jeweiligen Zeitraums.

(3) Die Deutsche Rentenversicherung Bund erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik ein Sicherheitskonzept für die Einrichtung des automatisierten Verfahrens, das insbesondere die nach § 78a des Zehnten Buches erforderlichen technischen und organisatorischen Maßnahmen enthalten muss. Wenn sicherheitserhebliche Änderungen am automatisierten Verfahren vorgenommen werden, das Sicherheitskonzept nicht mehr dem Stand der Technik entspricht oder dieses aus einem sonstigen Grund nicht geeignet ist, die Datensicherheit zu gewährleisten, spätestens jedoch alle vier Jahre, ist das Sicherheitskonzept im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik zu aktualisieren. Das Sicherheitskonzept ist der jeweiligen Aufsichtsbehörde unter Beifügung der Erklärung des Bundesamtes für Sicherheit in der Informationstechnik vorzulegen. Einrichtung und sicherheitserhebliche Änderungen des Verfahrens bedürfen der vorherigen Zustimmung der jeweiligen Aufsichtsbehörde. Die Zustimmung gilt als erteilt, wenn die Aufsichtsbehörde nicht innerhalb einer Frist von drei Monaten nach Vorlage des Antrags eine andere Entscheidung trifft. Die Aufsichtsbehörde kann den Betrieb des Verfahrens untersagen, wenn eine Aktualisierung nicht erfolgt.

SGB VI § 153 Umlageverfahren

(1) In der Rentenversicherung werden die Ausgaben eines Kalenderjahres durch die Einnahmen des gleichen Kalenderjahres und, soweit erforderlich, durch Entnahmen aus der Nachhaltigkeitsrücklage gedeckt.

(2) Einnahmen der allgemeinen Rentenversicherung sind insbesondere die Beiträge und die Zuschüsse des Bundes, Einnahmen der knappschaftlichen Rentenversicherung sind insbesondere die Beiträge und die Mittel des Bundes zum Ausgleich von Einnahmen und Ausgaben.

(3) Nach § 7f Abs. 1 Satz 1 Nr. 2 des Vierten Buches übertragene Wertguthaben sind nicht Teil des Umlageverfahrens. Insbesondere sind die aus der Übertragung und Verwendung von Wertguthaben fließenden und zu verwaltenden Mittel keine Einnahmen, Ausgaben oder Zahlungsverpflichtungen der allgemeinen Rentenversicherung.

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

SGB X

§ 79 Einrichtung automatisierter Verfahren auf Abruf

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung von Sozialdaten durch Abruf ermöglicht, ist zwischen den in § 35 des Ersten Buches genannten Stellen sowie mit der Deutschen Rentenversicherung Bund als zentraler Stelle zur Erfüllung ihrer Aufgaben nach § 91 Absatz 1 Satz 1 des Einkommensteuergesetzes und der Deutschen Rentenversicherung Knappschaft-Bahn-See, soweit sie bei geringfügig Beschäftigten Aufgaben nach dem Einkommensteuergesetz durchführt, zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist und wenn die jeweiligen Rechts- oder Fachaufsichtsbehörden die Teilnahme der unter ihrer Aufsicht stehenden Stellen genehmigt haben. Das Gleiche gilt gegenüber den in § 69 Absatz 2 und 3 genannten Stellen.

(1a) Die Einrichtung eines automatisierten Verfahrens auf Abruf für ein Dateisystem der Sozialversicherung für Landwirtschaft, Forsten und Gartenbau ist nur gegenüber den Trägern der gesetzlichen Rentenversicherung, der Deutschen Rentenversicherung Bund als zentraler Stelle zur Erfüllung ihrer Aufgaben nach § 91 Absatz 1 Satz 1 des Einkommensteuergesetzes, den Krankenkassen, der Bundesagentur für Arbeit und der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist, zulässig; dabei dürfen auch Vermittlungsstellen eingeschaltet werden.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Verfahrens auf Abruf kontrolliert werden kann. Hierzu haben sie schriftlich oder elektronisch festzulegen:

1.

Anlass und Zweck des Verfahrens auf Abruf,

2.

Dritte, an die übermittelt wird,

3.

Art der zu übermittelnden Daten,

4.

nach Artikel 32 der Verordnung (EU) 2016/679 erforderliche technische und organisatorische Maßnahmen.

(3) Über die Einrichtung von Verfahren auf Abruf ist in Fällen, in denen die in § 35 des Ersten Buches genannten Stellen beteiligt sind, die der Kontrolle des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Bundesbeauftragte) unterliegen, dieser oder diese, sonst die nach Landesrecht für die Kontrolle des Datenschutzes zuständige Stelle rechtzeitig vorher unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Sie hat mindestens bei jedem zehnten Abruf den Zeitpunkt, die abgerufenen Daten sowie Angaben zur Feststellung des Verfahrens und des für den Abruf Verantwortlichen zu protokollieren; die protokollierten Daten sind spätestens nach sechs Monaten zu löschen. Wird ein Gesamtbestand von Sozialdaten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Dateisystemen, die mit Einwilligung der betroffenen Personen angelegt werden und die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offen stehen.

SGB X

§ 80 Verarbeitung von Sozialdaten im Auftrag

(1) Die Erteilung eines Auftrags im Sinne des Artikels 28 der Verordnung (EU) 2016/679 zur Verarbeitung von Sozialdaten ist nur zulässig, wenn der Verantwortliche seiner Rechts- oder Fachaufsichtsbehörde rechtzeitig vor der Auftragserteilung

1.

Auszug der Rechtsgrundlagen für die Deutsche Rentenversicherung im Rahmen der Betrachtung als kritische Infrastruktur

den Auftragsverarbeiter, die bei diesem vorhandenen technischen und organisatorischen Maßnahmen und ergänzenden Weisungen,

2.

die Art der Daten, die im Auftrag verarbeitet werden sollen, und den Kreis der betroffenen Personen,

3.

die Aufgabe, zu deren Erfüllung die Verarbeitung der Daten im Auftrag erfolgen soll, sowie

4.

den Abschluss von etwaigen Unterauftragsverhältnissen

schriftlich oder elektronisch anzeigt. Soll eine öffentliche Stelle mit der Verarbeitung von Sozialdaten beauftragt werden, hat diese rechtzeitig vor der Auftragserteilung die beabsichtigte Beauftragung ihrer Rechts- oder Fachaufsichtsbehörde schriftlich oder elektronisch anzuzeigen.

(2) Der Auftrag zur Verarbeitung von Sozialdaten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt.

(3) Die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist nur zulässig, wenn

1.

beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder

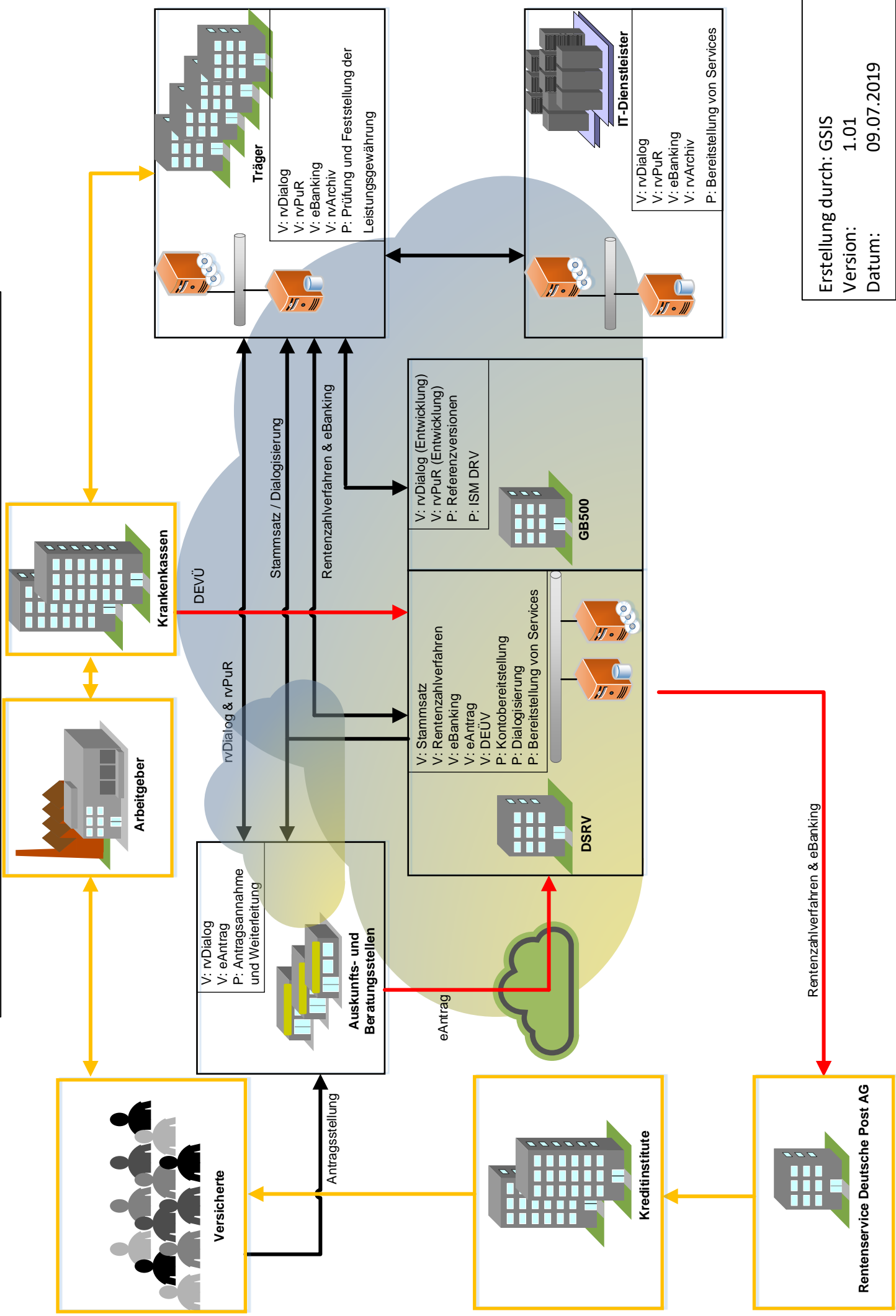
2.

die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.

(4) Ist der Auftragsverarbeiter eine in § 35 des Ersten Buches genannte Stelle, gelten neben den §§ 85 und 85a die §§ 9, 13, 14 und 16 des Bundesdatenschutzgesetzes. Bei den in § 35 des Ersten Buches genannten Stellen, die nicht solche des Bundes sind, tritt anstelle des oder der Bundesbeauftragten insoweit die nach Landesrecht für die Kontrolle des Datenschutzes zuständige Stelle. Ist der Auftragsverarbeiter eine nicht-öffentliche Stelle, unterliegt dieser der Aufsicht der gemäß § 40 des Bundesdatenschutzgesetzes zuständigen Behörde.

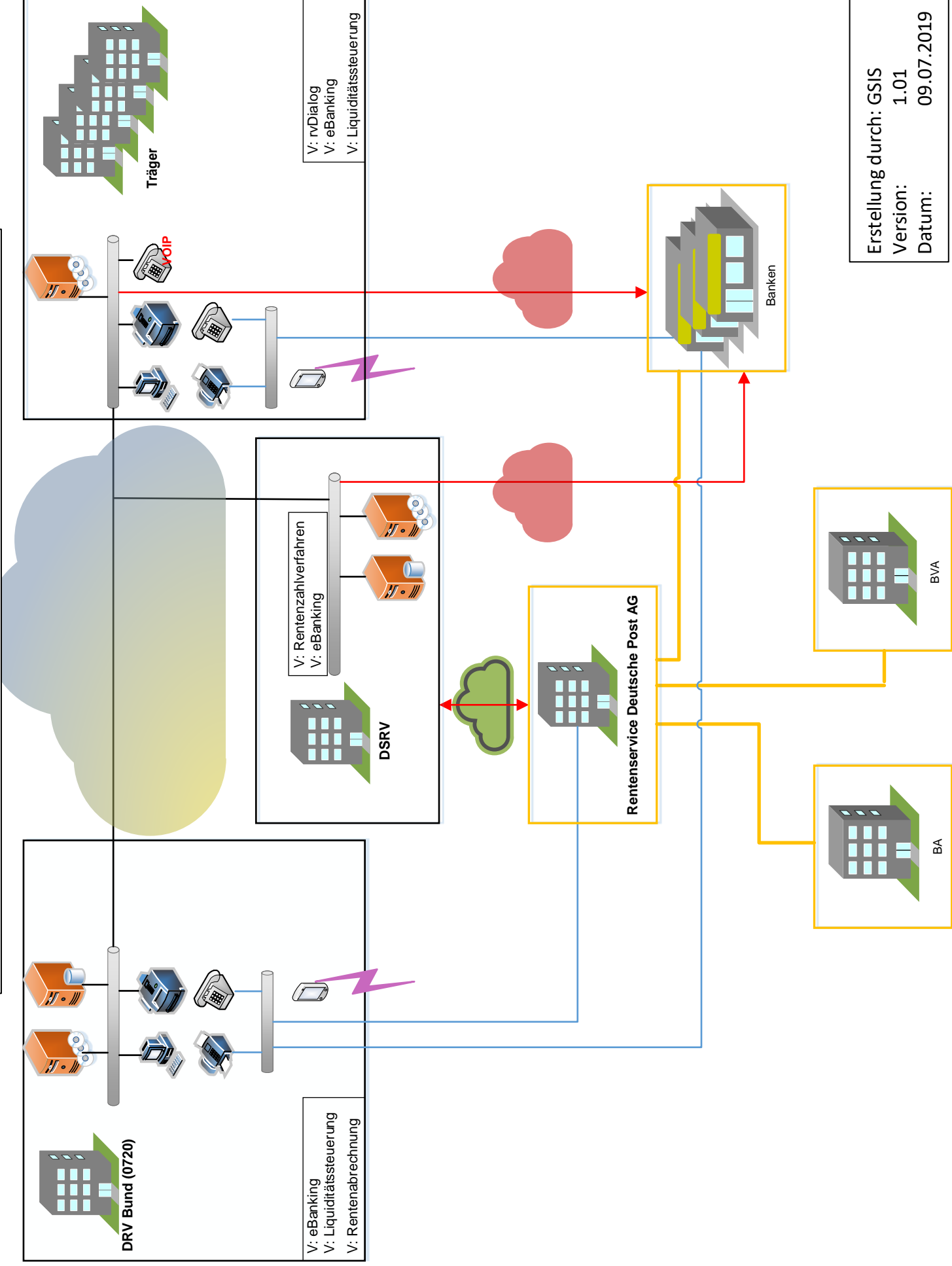
(5) Absatz 3 gilt nicht bei Verträgen über die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann. Die Verträge sind bei zu erwartenden oder bereits eingetretenen Störungen im Betriebsablauf unverzüglich der Rechts- oder Fachaufsichtsbehörde mitzuteilen.

Leistungserbringung der Deutschen Rentenversicherung















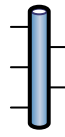
Erstellung durch: GSIS
 Version: 1.01
 Datum: 09.07.2019

Liquiditätsbereitstellung der Deutschen Rentenversicherung



Erstellung durch: GSIS
 Version: 1.01
 Datum: 09.07.2019

Legende

Symbol	Bedeutung	Symbol	Bedeutung
	DRV WAN		Anwendungsserver
	Netze des Bundes		Datenbankserver
	Externes Datennetz (z. B. Internet)	P:	Prozess(e) xxx
	LAN (Verbund)	V:	Verfahren xxx
	Externer IT-Verbund (nicht betrachtet)		
	Externe Datenstrecke (nicht betrachtet)		
	DRV interne Datenstrecke		
	Verschlüsselte Datenstrecke		
	Kommunikations Datenstrecke		
	Mobilfunk		
	Separiertes Datennetz (z.B. VLAN)		

Erstellung durch: GSIS
Version: 1.01
Datum: 09.07.2019