Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

Bundesunmittelbare

Sozialversicherungsträger

nachrichtlich:

Bundesministerium für Arbeit und Soziales
Referat Ib 5
53107 Bonn

Bundesministerium für Gesundheit
Referat 217
53107 Bonn

Bundesministerium für Ernährung
und Landwirtschaft
Referat 724
Rochusstraße 1
53123 Bonn

Minister/-innen und
Senatoren/-innen für Arbeit,
Gesundheit und Soziales der Länder

GKV-Spitzenverband
Reinhardstraße 28
10117 Berlin

Deutsche Gesetzliche
Unfallversicherung e.V.
Glinkastraße 40
10117 Berlin

Deutsche Rentenversicherung Bund
Stabsstelle Koordinierung und Compliance
Ruhrstraße 2
10709 Berlin

- Versand erfolgt nur per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1615
FAX +49 228 619 1874

referat511@bas.bund.de
www.bundesamtsozialesicherung.de

BEARBEITER(IN) FRAU DR. SCHERER

22. Juni 2020

AZ **511 – 3700 – 1738/2007**
(bei Antwort bitte angeben)

Anforderungen an IT-gestützte Verfahren des Rechnungswesens zur Ersetzung von Schriftformerfordernissen

Veröffentlichung von Hinweisen zur Erstellung einer Dienstanweisung nach § 40 Abs. 5, § 41a der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV)

Sehr geehrte Damen und Herren,

seit dem 1. Januar 2019 ermöglichen Sozialversicherungs-Rechnungsverordnung (SVRV) und SRVwV, bei IT-gestützter, automatisierter Feststellung und Anordnung von Zahlungen und Buchungen auf den kostenintensiven Einsatz qualifizierter elektronischer Signaturen zur Ersetzung der Schriftform zu verzichten (§ 7 Abs. 3 und 5 SVRV, §§ 19 Abs. 5 i. V. m. 40 Abs. 5, 41 Abs. 1 Satz 3, 41a SRVwV). Voraussetzung hierfür ist, dass dokumentierte, hinreichend getestete und freigegebene Programme eingesetzt werden. Zu diesem Zweck ist eine Verfahrensdokumentation einschließlich einer Gefährdungsanalyse und eines Ordnungsmäßigkeitskonzeptes zu erstellen; die Details sind in einer Dienstanweisung zu regeln.

An das Bundesamt für Soziale Sicherung wurden Anfragen zu den erforderlichen Änderungen in der Dienstanweisung nach § 17 SVRV, § 44 Abs. 4 SRVwV herangetragen. Da alle Sozialversicherungsträger sowie die weiteren Institutionen, die die SVRV/SRVwV anwenden, davon betroffen sind, veröffentlichen wir nachfolgend allgemeine Hinweise zur Erstellung der geforderten Dokumentationen in Form einer „Arbeitshilfe“. Bei der Zusammenstellung der Hinweise haben wir uns insbesondere an folgenden parallelen Vorschriften und Veröffentlichungen orientiert:

- „Grundsätze ordnungsgemäßer Buchführung bei Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes“ (GoBIT-HKR)
- „IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1),
- BMF, „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“, 28. November 2019 (GoBD).

Sollten Sie zu der „Arbeitshilfe“ vor dem Hintergrund der eigenen betrieblichen Praxis Rückfragen, Anregungen oder Verbesserungsvorschläge haben, stehen wir für eine Diskussion gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag
Reiner Müller

Anlage

ARBEITSHILFE ZU § 40 ABS. 5, § 41A SRVWV

I. F.A.Q.-Liste

1. Können wir vollständig auf qualifizierte elektronische Signaturen verzichten?

Aus der SRVwV ergeben sich diverse Schriftformerfordernisse. Bislang konnte nach § 41 Abs. 1, Satz 1 SRVwV die Unterschrift ausschließlich durch eine qualifizierte elektronische Signatur (qeS) ersetzt werden. Seit Januar 2019 gilt nach Satz 3 eine Ausnahme für die Feststellung von Belegen und die Anordnung von Zahlungen und Buchungen, wenn diese unter Einsatz IT-gestützter Verfahren erfolgen, die wiederum die Anforderungen des § 40 und § 41a SRVwV erfüllen. Hintergrund ist, dass IT-gestützte Prüf- und Feststellungsverfahren weniger fehleranfällig als manuelle Verfahren sind, wenn die technischen Voraussetzungen für einen hohen Integritätsschutz der Daten und Prozesse gegeben sind.
Folglich können die Feststellung der sachlichen und rechnerischen Richtigkeit und die Zahlungs- bzw. Buchungsanordnung ohne Einsatz einer qeS erfolgen, vorausgesetzt, dass diese beiden Vorgänge IT-gestützt erfolgen und dass die eingesetzten IT-Verfahren den Anforderungen von §§ 40, 41a SRVwV genügen.

2. Wir möchten, soweit wie möglich, auf den Einsatz qualifizierter elektronischer Signaturen verzichten. Was ist zu tun?

Neben der Kassenordnung nach § 3 SVRV, § 44 Abs. 3 SRVwV muss vor allem die Dienstanweisung (im Folgenden: DA) zur Sicherheit des Verfahrens nach § 17 SVRV, § 44 Abs. 4 SRVwV angepasst werden. In der Regel existiert bereits eine DA zur Sicherheit des Verfahrens nach § 17 SVRV mit den in § 40 SRVwV auch bisher schon aufgezählten Mindestinhalten. Zusätzlich sind die in § 40 Absatz 5 SRVwV beschriebenen Detailregelungen in die DA aufzunehmen, die sich aus Verfahrensdokumentation, Gefährdungsanalyse und Ordnungsmäßigkeitskonzept gemäß Anlage 9 zu § 40 SRVwV ergeben. Die geforderten Ergänzungen setzen voraus, dass **trägerindividuelle** Maßnahmen zur Gewährleistung der Einhaltung der Grundsätze ordnungsmäßiger Buchführung beim Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen festgelegt werden. Die spezifischen Umstände

der Verarbeitung bei dem jeweiligen Sozialversicherungsträger, wie z.B. die eingesetzte Software, der konkrete Informationsverbund, organisatorische Gegebenheiten, wirtschaftliche und (sicherheits-)strategische Vorgaben müssen hierbei berücksichtigt werden. Es obliegt dem Sozialversicherungsträger im Rahmen seiner Einschätzungsprärogative, die erforderlichen Festlegungen zu treffen.

3. Bei uns bleibt alles wie bisher – besteht durch die Änderungen von SVRV und der SRVwV trotzdem Handlungsbedarf?

Zu beachten ist, dass durch die Neufassung von § 40 Abs. 2 SRVwV und den Verweis auf Art. 32 Datenschutz-Grundverordnung (DS-GVO) die Neuerungen im Datenschutzrecht nachvollzogen wurden. Im Rahmen des Datenschutzmanagements sollte daher ein möglicher Aktualisierungsbedarf geprüft werden.
Spätestens bei der Einführung neuer Verfahren, bei Verfahrensänderungen oder bei Verzicht auf qualifizierte elektronische Signaturen im Rahmen von automatisierter Feststellung und/oder Anordnung von Zahlungen und Buchungen müssen nach § 40 Abs. 4 und Abs. 5 SRVwV die von der neu gefassten Anlage 9 zu § 40 SRVwV formulierten Anforderungen an die Dokumentation erfüllt werden. Hierzu gehört insbesondere die Durchführung einer eigenen Gefährdungsanalyse, in der die Risiken der Verarbeitung speziell für das Rechnungswesen und die Haushaltswirtschaft betrachtet werden.

4. Die von uns eingesetzten Systeme und Lösungen zur elektronischen Buchführung, Zahlung und Rechnungslegung sind umfassend im Hinblick auf Datenschutz und Informationssicherheit geprüft und dokumentiert worden. Reicht das nicht?

Im Verhältnis zu den Anforderungen des Datenschutzes und der Informationssicherheit ergeben sich aus den Vorschriften zur Verfahrenssicherheit nach SVRV und SRVwV zusätzliche Anforderungen, die die spezifischen Gefährdungen für die Ordnungsmäßigkeit der Buchführung bei elektronischer Verarbeitung im Fokus haben. Die technischen und organisatorischen Maßnahmen (TOMs) des Datenschutzes und der Informationssicherheit müssen also entsprechend ergänzt werden. Die Regelungsbereiche überschneiden sich teilweise. Da für Zahlungs-, Buchführungs- und Rechnungslegungssysteme die Vollständigkeit und Richtigkeit der Daten und damit der Schutz vor unbemerkter oder unberechtigter Veränderung eine besondere Rolle spielt, gibt es insbesondere zu dem auch von Datenschutz und Informationssicherheit geforderten Integritätsschutz eine große Schnittmenge. Überschneidungen

gibt es jedoch auch in den Bereichen Vertraulichkeit und Verfügbarkeit. Daten dürfen nicht unberechtigt weitergegeben oder veröffentlicht werden und es muss sichergestellt sein, dass die Buchführung in angemessener Frist lesbar gemacht werden kann und aufbewahrungspflichtige Unterlagen verfügbar sind.

5. Heißt das, dass die aufwendigen Prüfungen aus Datenschutz- und Informationssicherheits-Sicht wiederholt werden müssen?

Das ist nicht zwingend. Zur Sicherstellung von Datenschutz und Informationssicherheit werden die bekannten Methodiken nach Standard-Datenschutz-Modell[1] und BSI-Grundschutz[2] angewendet. Schutzbedarfsermittlung bzw. Risikoanalyse und ggf. Datenschutzfolgenabschätzung analysieren die konkrete Verarbeitungssituation und bestehende Gefährdungen mit dem Ziel, die Gewährleistungsziele der Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettung, Transparenz und Intervenierbarkeit durch geeignete Maßnahmen so abzusichern, dass ein den Umständen der Verarbeitung angemessenes Schutzniveau erreicht wird. Während die Informationssicherheit Gefährdungen für die Organisation selbst im Blick hat, legt der Datenschutz den Fokus auf Gefährdungen der von der Datenverarbeitung betroffenen Personen. Für weiterführende Hinweise zu den Anforderungen an Vorgehensweise und Dokumentation wird auf das Standard-Datenschutz-Modell der Datenschutz-Aufsichtsbehörden und die Grundschutz-Standards und das Grundschutz-Kompendium des BSI verwiesen. Wenn zumindest Teile von Buchführung und Rechnungslegung auch bisher schon IT-gestützt erledigt wurden und die Vorkehrungen zum Datenschutz und zur Sicherstellung der Informationssicherheit auf einem aktuellen Stand sind, kann auf die vorhandenen Dokumentationen aufgebaut werden.

Die Gefährdungsanalyse nach Anlage 9 zu § 40 SRVwV kann unabhängig von der Risikoanalyse aus Sicht von Datenschutz und Informationssicherheit durchgeführt und dokumentiert werden, setzt aber zwingend voraus, dass grundlegende Sicherheitsanforderungen zum Schutz des IT-Systems auf Organisations-, Betriebs- und Infrastrukturebene erfüllt werden. Der Fokus der Gefährdungsanalyse liegt auf Gefährdungen für die Ordnungsmäßigkeit der Buchführung. Besondere Aufmerksamkeit richtet sich hierbei deshalb auf IT-anwendungs-

[1] AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.), „Das Standard-Datenschutzmodell, eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“, Version 2.0, von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 5. bis 7. November 2019 in Trier beschlossen.

[2] Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de/grundschutz .

bezogene Anforderungen. Hinweise zu den bei der spezifischen Gefährdungsanalyse zu berücksichtigenden Aspekten und zu möglichen TOMs werden unter II. aufgeführt.

Es wird empfohlen, die Ergebnisse der jeweiligen Analysen aus Datenschutz- und Informationssicherheitssicht sowie aus Buchführungs- und Rechnungslegungssicht, also jeweils ein Set von TOMs, in den Regelungen der DA nach dem Maximalprinzip zusammenzuführen, um eine Mehrfachregelung derselben Inhalte und Widersprüche zu vermeiden. Die jeweils strengste Anforderung aus den drei Bereichen sollte umgesetzt werden (Beispiel: Ergebnis der Datenschutz-Analyse ist, dass ein Berechtigungskonzept zu erstellen ist, um Vertraulichkeit und Integrität der Daten zu schützen. Die Gefährdungsanalyse für Rechnungswesen und Haushaltswirtschaft ergibt, dass ein Berechtigungskonzept zusätzlich die Angaben enthalten muss, die die Ordnungsmäßigkeit sicherstellen. Im Ergebnis muss sowohl ein Berechtigungs- als auch ein Ordnungsmäßigkeitskonzept erstellt werden.).

6. Welche Informationsgrundlage benötigen wir, um eine Gefährdungsanalyse durchführen zu können?

Grundlage einer Gefährdungsanalyse muss die von Anlage 9 zu § 40 SRVwV geforderte, aussagekräftige Verfahrensbeschreibung sein.
Die Verfahrensdokumentation nach Anlage 9 zu § 40 SRVwV hat mindestens folgenden Inhalt:

- eine Beschreibung der sachlogischen Lösung (= Darstellung der fachlichen Aufgabe aus der Sicht des Anwenders – generelle Aufgabenstellung, Beschreibung der Anwenderoberflächen für Ein- und Ausgabe einschließlich der manuellen Arbeiten, Beschreibung der Datenbestände, Beschreibung von Verarbeitungsregeln, Beschreibung des Datenaustausches (Datenträgeraustausch/Datentransfer), Beschreibung der maschinellen und manuellen Kontrollen, Beschreibung der Fehlermeldungen und der sich aus Fehlern ergebenden Maßnahmen, Schlüsselverzeichnisse, Schnittstellen zu anderen Systemen)
- eine Beschreibung der programmtechnischen Lösung (= Umsetzung der sachlogischen Forderungen in Programmen inklusive Dokumentation von Programmänderungen)
- eine Beschreibung, wie die Programmidentität gewahrt wird
- Beschreibung, wie die Integrität von Daten gewahrt wird
- Arbeitsanweisungen für den Anwender

- ein differenziertes Rollen- und Berechtigungskonzept zu den relevanten Zahlungsfunktionen,
- eine Gefährdungsanalyse,
- ein Ordnungsmäßigkeitskonzept.

Sachlogische und programmtechnische Beschreibung können in der Regel nicht ohne Rückgriff auf Herstellerdokumentationen erstellt werden. Die Herstellerdokumentation muss zusätzlich durch eine Beschreibung der spezifischen Anpassungen des Anwenders (z.B. Parametrisierungen, Konfiguration) und die Dokumentation des eingerichteten internen Kontrollsystems ergänzt werden. Da auch eine Risikoanalyse aus Datenschutz- oder Informationssicherheitssicht eine Verfahrensbeschreibung voraussetzt, empfiehlt es sich zu prüfen, welche der bereits vorhandenen Dokumentationen für die Gefährdungsanalyse nutzbar gemacht werden können. Bereits im Rahmen der Beschaffung von IT-Lösungen ist darauf zu achten, dass der Hersteller bzw. Bereitsteller von Software zusichert, die Grundlagen für die Verfahrensbeschreibung nach Anlage 9 zu § 40 SRVwV auf Verlangen jederzeit bereitzustellen.

Es wird empfohlen, die eingesetzten IT-Lösungen regelmäßig durch externe Dritte (Sachverständige) prüfen zu lassen bzw. bei der Zusammenarbeit mit Dienstleistern sich Berichte und Zertifikate solcher Prüfungen vorlegen zu lassen.

7. Wir arbeiten mit externen Dienstleistern zusammen, die z.B. das Hosting übernehmen oder die Software-Lösungen bereitstellen. Was ist zu beachten?

Auch bei Einsatz eines Dienstleisters bleibt der Sozialversicherungsträger für die Einhaltung der SVRV und SRVwV verantwortlich, § 19 SVRV, § 42 SRVwV. Daher müssen mit Dienstleistern geeignete vertragliche Vereinbarungen getroffen werden, in denen der Dienstleister sich verpflichtet, die Vorgaben der SVRV und SRVwV sowie die von dem jeweiligen Träger festgelegten Anforderungen zum Schutz der Ordnungsmäßigkeit der Buchführung zu erfüllen. Ist der Dienstleister der Hersteller oder Bereitsteller der Software, hat er zuzusichern, dass Dokumentationen wie die Beschreibungen der sachlogischen und programmtechnischen Lösung (technische Systemdokumentation), Betriebs- und Anwenderhandbücher etc. auf Verlangen jederzeit bereitgestellt werden. Es kann sinnvoll sein, Unterstützungsleistungen für die Durchführung der Gefährdungsanalyse zu fordern. Dienstleister sind zudem auf die Prüfrechte des Sozialversicherungsträgers sowie der Aufsichtsbehörden nach § 19 SVRV, § 42 SRVwV hinzuweisen. Die Einhaltung von SVRV und SRVwV durch den Dienstleister ist vom Träger mindestens einmal jährlich zu prüfen.

II. Gefährdungsanalyse: Hinweise zu Schutzzielen und möglichen TOMs

Wenn die Grundsätze von Rechnungswesen und Haushaltswirtschaft durch Fehler oder Missbrauch bei der elektronischen Verarbeitung verletzt werden können, bestehen Gefährdungen. Aus der Betrachtung der möglichen Auswirkungen von Fehlern oder Missbrauch und deren Eintrittswahrscheinlichkeit sind diese Ereignisse einem von drei Risikograden zuzuordnen (z.B. normal, substanziell, hoch). Anlage 9 zu § 40 SRVwV enthält Hinweise zur Risikoeinstufung. Demnach sind höhere Risiken jedenfalls dann anzunehmen, wenn

- Geschäftsvorfälle zu wiederkehrenden Zahlungen führen und im voraussichtlichen Anspruchszeitraum den Betrag von 7.500 Euro übersteigen,
- Geschäftsvorfälle zu Zahlungen auf unbestimmte Zeit führen,
- Einmalzahlungen den Betrag von 2.500 Euro übersteigen,
- auf Forderungen verzichtet wird (z. B. Niederschlagung, Erlass),
- Verwahrgelder ausgezahlt werden oder
- Beträge als Vorschüsse gezahlt werden.

Bestehende Risiken müssen durch TOMs entsprechend dem Risikograd und der hierfür zu treffenden Schutzmechanismen beherrscht werden. Bei der Auswahl der TOMs ist zwischen Aufwand/Kosten und Nutzen für die Erhöhung der Verfahrenssicherheit abzuwägen. Die verbleibenden Restrisiken sind aussagekräftig und vor dem Hintergrund des jeweiligen Risikograde nachvollziehbar und plausibel zu dokumentieren.

Im Folgenden wird anhand der **Grundsätze ordnungsmäßiger Buchführung (§ 10 SVRV)** aufgezeigt, wie bzw. mit welchen TOMs (bei den genannten TOMs handelt es sich nicht um konkrete Vorgaben, sondern lediglich um Beispiele) den spezifischen Gefährdungen **bei elektronischer Aufzeichnung und Verarbeitung** begegnet werden kann. Die Ausführungen können eine eigene Gefährdungsanalyse des Trägers nicht ersetzen, können aber der Orientierung bei der Durchführung einer Gefährdungsanalyse dienen.

1. Nachvollziehbarkeit und Nachprüfbarkeit, Vollständigkeit

Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- oder Aufzeichnungsverfahren muss nachvollziehbar sein. Alle Geschäftsvorfälle müssen also in ihrer Entstehung und Abwicklung vollständig für die gesamte Dauer der Aufbewahrungsfrist und in jedem Verfahrensschritt lückenlos verfolgbar sein.

Unentbehrlich ist daher eine aussagekräftige und vollständige Verfahrensdokumentation. Daten, IT-Anwendungen und IT-Infrastruktur dürfen nur in einem festgelegten Zustand nach Durchlaufen von Test- und Freigabeverfahren eingesetzt werden. Die Regeln für Generierung, Steuerung und Kontrolle von automatisierten Prozessen und Buchungen müssen aus der Verfahrensdokumentation hervorgehen. Für Änderungen an automatisierten Berechnungsprozessen sind Autorisierungen und Dokumentation vorzusehen.

Darüber hinaus bieten z.B. folgende TOMs die Möglichkeit, die Vollständigkeit und Lückenlosigkeit der Erfassung von Geschäftsvorfällen sicherzustellen: Plausibilitätskontrollen bei Dateneingaben, Erfassungskontrollen, inhaltliche Plausibilitätskontrollen, automatisierte Vergabe von Datensatznummern, Lückenanalyse oder Mehrfachbelegungsanalyse bei Belegnummern.

2. Zeitgerechte Buchungen und Aufzeichnungen; zeitliche und sachliche Ordnung

Geschäftsvorfälle sollen möglichst unmittelbar nach Entstehung erfasst und laufend in zeitlicher Reihenfolge gebucht werden (Zeitbuch/Journal). Wenn es zeitliche Abstände zwischen Entstehung und Erfassung von Geschäftsvorfällen gibt, sind Maßnahmen zur Sicherung der Vollständigkeit der Aufzeichnungen zu treffen.
Sobald elektronische Aufzeichnungen Belegfunktionen erfüllen, dürfen unprotokollierte Änderungen und Löschungen nicht mehr möglich sein (Revisionssicherheit). Mit elektronischen Aufzeichnungen sind sowohl originär elektronisch erstellte Belege/Datensätze als auch elektronisch erfasste konventionelle Belege (d.h. originär papiergebundene/körperliche Belege) gemeint. Revisionssicherheit muss auch dann gewährleistet sein, wenn die Erfassung in vorgelagerten IT-Systemen (im Folgenden: Vorsystemen) erfolgt. Durch technische Maßnahmen (z.B. Kontroll- und Abstimmungsverfahren) muss sichergestellt sein, dass die Identität der im Vor- oder Nebensystem gespeicherten Buchungen mit den im Hauptsystem vorhandenen Buchungen übereinstimmen.
Es sollten Erfassungs-, Übertragungs- und Verarbeitungskontrollen durchgeführt und dokumentiert werden.

Sachbuch/Konten müssen nach systematischen Ordnungsprinzipien unter Beachtung des jeweiligen Kontenrahmens geführt werden, in sachlicher Gliederung darstellbar sein und innerhalb angemessener Frist lesbar gemacht werden können.
Die genutzte Software muss daher in der Lage sein, Vorgänge sowohl in zeitlicher Reihenfolge als auch sachlich gegliedert darzustellen. Werden mehrere Systeme verwendet oder innerhalb desselben Systems unterschiedliche Ordnungskriterien, muss die Zuordnung jederzeit möglich sein (z.B. Mappingtabellen, Verlinkungen, Schlüsselfelder).

3. Unveränderbarkeit bzw. Nachvollziehbarkeit von Änderungen

Die Unveränderbarkeit von Daten, Datensätzen und elektronischen Dokumenten und das Ziel der Revisionssicherheit kann am besten durch ein Maßnahmenbündel nach dem aktuellen Stand der Technik, ergänzt um organisatorische Maßnahmen erreicht werden. Die zur Verfügung stehenden technischen Lösungen sind vielfältig und müssen in der Regel durch organisatorische Maßnahmen flankiert werden. Denkbar sind z.B. hardwareseitig Lösungen durch den Einsatz von unveränderbaren und fälschungssicheren Datenträgern, softwareseitige Lösungen z.B. durch den Einsatz von Sicherungen, Sperren, Festschreibungen, Löschmerkern, automatischen Protokollierungen, Historisierungen, Versionierungen und/oder Zugriffsschutzverfahren und Berechtigungskonzepte.

Erfassungen, die Belegfunktionen erfüllen, müssen den Namen des Erfassenden und den Zeitpunkt der Erfassung aufzeichnen. Jede Ersetzung, Veränderung und Löschung von Aufzeichnungen muss so protokolliert werden, dass neben der Tatsache der Änderung der vorausgegangene Inhalt weiterhin feststellbar ist. Bei programmgesteuerten Aufzeichnungen müssen daher auch Änderungen an den Einstellungen und der Parametrisierung der Software protokolliert werden. Besondere Vorsicht ist bei der Änderung von Stammdaten angezeigt. Hier muss die Eindeutigkeit von Verknüpfungen ggf. durch die Historisierung von Stammdaten mit Gültigkeitsangaben sichergestellt werden, wenn Stammdatenänderungen nicht ganz ausgeschlossen werden können.

4. Belegfunktion

Werden konventionelle Belege ersetzt, muss die ordnungsgemäße Anwendung des jeweiligen Verfahrens nachgewiesen werden. Hierzu muss die Verfahrensbeschreibung folgende Angaben enthalten: Dokumentation der programminternen Vorschriften zur Generierung der Buchungen, Nachweis oder Bestätigung, dass die in der Dokumentation enthaltenen Vorschriften einem autorisierten Änderungsverfahren unterlegen haben (u.a. Zugriffsschutz, Versionsführung, Test- und Freigabeverfahren), Nachweis der Anwendung des genehmigten Verfahrens, Nachweis der tatsächlichen Durchführung der einzelnen Buchungen.

Es muss festgelegt sein, wie elektronische Unterlagen erfasst, empfangen, verarbeitet, ausgegeben, aufbewahrt und gegen Verlust gesichert werden. Eingehende elektronische Unterlagen sind im Rahmen der sachlichen Feststellung auf Integrität und Authentizität zu prüfen. Aufbewahrungspflichtige elektronische Unterlagen sind in Form der Erstellung oder der Übernahme unverändert aufzubewahren.

Elektronische Belege müssen eine eindeutige Belegnummer erhalten (z.B. durch automatische Vergabe – über einen Index, Paginiernummer, Dokumenten-ID etc.). Zu den zwingenden Angaben gehören außerdem das Belegdatum mit dem Zeitpunkt der Erfassung, dem verantwortlichen Aussteller und dem Erfasser. Der Umfang der von den beteiligten Personen jeweils wahrgenommenen Verantwortung muss ersichtlich sein. Elektronische Belege sollen durch Verbindung mit einem Datensatz oder durch eine eindeutige elektronische Verknüpfung (z.B. eindeutiger Index, Barcode) mit Angaben zur Kontierung verknüpft werden. Damit der Zusammenhang der einzelnen Unterlagen zu einem Geschäftsvorfall gewahrt bleibt, muss es für die Zuordnung zwischen dem einzelnen Beleg und der dazugehörigen Aufzeichnung oder Buchung Zuordnungsmerkmale (z.B. Index, Paginiernummer, Dokumenten-ID) und Identifikationsmerkmale (z.B. Such- und Filtermöglichkeiten der Belegablage) geben, die in die Bücher oder Aufzeichnungen übernommen werden. Wird nicht mit Dokumenten, sondern mit Datensätzen belegt (elektronische Meldungen), müssen diese vollständig gespeichert und aufbewahrt werden.
Für die Umwandlung von Papierunterlagen in elektronische Unterlagen durch einen Erfassungsvorgang (z.B. Scannen, Fotografieren) muss sichergestellt sein, dass Original und elektronisches Dokument (z.B. Scan, Bild) übereinstimmen und dass die weitere Bearbeitung ausschließlich mit der elektronischen Unterlage erfolgt. Unprotokollierte Änderungen und Löschungen dürfen nicht mehr möglich sein (Revisionssicherheit). Das Verfahren muss dokumentiert werden (Erfassungsberechtigungen, Zeitpunkt des Erfassens, Gegenstand des Erfassens, Qualitätssicherung hinsichtlich Lesbarkeit und Vollständigkeit, Fallgruppen für Vernichtung bzw. Aufbewahrung von Originalunterlagen, Zuordnung der elektronischen Unterlage zu einem Geschäftsvorfall, Protokollierung von Fehlern).

Es wird darauf hingewiesen, dass neben den hier aufgeführten spezifischen Anforderungen für die Sicherheit von Zahlungsverkehr, Rechnungslegung und Buchführung die allgemeinen Anforderungen an die Beweiskraft von Dokumenten im Verwaltungsverfahren zu beachten sind, sofern keine bereichsspezifischen Erleichterungen gelten. Daher empfehlen wir, bei der Umwandlung von konventionellen (Papier-)Belegen in elektronische Dokumente die Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR RESISCAN (BSI TR 03138) zu beachten. Die Entscheidung über den Umsetzungsgrad dieser Vorgaben sollte auf einer trägerspezifischen Risikoanalyse für die unterschiedlichen Belegarten basieren, bei der auch Wirtschaftlichkeitsaspekte beachtet werden. Hinweise zu Anforderungen und praktischer Umsetzung können dem „Leitfaden Elektronische Kommunikation der Prüfdienste“, Punkt 3.2 entnommen werden, der auf der Homepage des Bundesamtes für Soziale Sicherung abrufbar ist:

https://www.bundesamtsozialesicherung.de/de/themen/krankenversicherung/pruefdienst-kranken-und-pflegeversicherung/ .

5. Aufbewahrung

Art und Umfang der Archivierung muss festgelegt werden. Zusätzlich zu den Belegen müssen mindestens der Name des Archivierenden und der Zeitpunkt der Archivierung gespeichert werden. Neben Regelungen zur Aufbewahrung der eigentlichen Bücher und Belege muss die Aufbewahrung der Unterlagen über den Aufbau der Datenträger und die Programmdokumentation einschließlich Testunterlagen über die Programme, die zur maschinellen Speicherung verwendet werden, geregelt werden (§ 35 Abs. 4 SRVwV).

Alle Aufbewahrungsregelungen und Fristen sollten in einem Archivierungs- und Löschkonzept geregelt werden. Die Aufbewahrungsfristen für revisionssichere Archivierung von Buchführungsunterlagen ergeben sich aus § 35 SRVwV. Ebenso sind betriebliche Bestimmungen des Anwenders hinsichtlich der Datensicherheit (z.B. Datensicherungskonzept) und des Datenschutzes (z.B. Speicherung nur auf Servern in Deutschland) über die Lebensdauer des Archives sicherzustellen und zu beachten. Die Datensätze müssen während der Aufbewahrungsfrist für Prüfungen jederzeit lesbar gemacht werden können und auffindbar sein. Der Zugriff auf die archivierten Daten ist in einem Benutzerkonzept festzulegen. Administrationsrechte mit der Möglichkeit der Veränderung/Löschung von Daten sind restriktiv zu vergeben. Der Zugriff sowie die Veränderbarkeit von Daten sind zu dokumentieren. Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist. Medienbrüche zwischen einzelnen Prozessschritten oder Prozessen vom Eingang/Antrag bis zur Langzeitspeicherung/Archivierung sollen vermieden werden. Neben Regelungen zur Aufbewahrung von Daten muss die Aufbewahrung von Programm- bzw. Verfahrensdokumentation geregelt werden.

6. Interne Kontrollen

Für folgende Bereiche empfiehlt es sich, interne Kontrollen einzurichten und dokumentiert auszuüben:

- Programmidentität, d.h. Übereinstimmung der tatsächlich eingesetzten Programme mit den Anforderungen in der Verfahrensdokumentation (beschriebenes Freigabeverfahren mit Freigabeerklärung und Testdatenbeständen)
- Umsetzung des Berechtigungskonzepts (tatsächlicher Zugang und Zugriff, Schnittstellen, Nachweis der Einhaltung des Verfahrens zur Vergabe von Berechtigungen)

- Umsetzung des Ordnungsmäßigkeitskonzeptes (z.B. Funktionstrennungen, Vier-Augen-Prinzip, Nachweis der Durchführung der vorgesehenen Stichprobenkontrollen bei automatisierten Verfahrensabläufen etc.)
- Erfassung- und Eingabe (Fehlerhinweise, Plausibilitätsprüfungen, Abgleiche, Plausibilitätskontrollen)
- Umsetzung der Maßnahmen zur Verhinderung von Verfälschung von Daten, Dokumenten oder Programmen.

III. Checkliste Inhalt der DA

Die DA (oder ihre Anlagen) enthält Regelungen zu…	√
Geltungsbereich	☐
Bezugnahme auf gesetzliche Regelungen, Verordnungen und Verwaltungsvorschriften	☐
ggf. Hinweis auf ergänzend zu beachtende interne Regelungen (z.B. Sicherheitsleitlinie, Datensicherungskonzept, Kryptokonzept etc.)	☐
Zuständigkeiten (auch für die vorgelagerte Gefährdungsanalyse für Zahlungsverkehr, Rechnungslegung und Buchführung sowie für die Schutzbedarfsfeststellung bzw. Risikoanalyse aus Informationssicherheits- und Datenschutzsicht)	☐
Regelungen zum Einsatz von Dienstleistern (§ 19 SVRV)	☐
Verweis auf alle Anlagen	☐
Maßnahmen zur Sicherheit bei der Datenfernübertragung und digitalen Aufzeichnung	☐
Datenträger und Datenformate	☐
Einsatz von elektronischen Signaturen	☐
Regelungen zum Scanverfahren	☐
Verfügbarkeitsanforderungen	☐
TOMs* zur Sicherstellung von Datenschutz, Datensicherheit und der Einhaltung der Grundsätze ordnungsmäßiger Buchführung (s.o. unter II.), insb. zu - Datenminimierung (z.B. Berechtigungskonzept, Löschkonzept etc.) - Vertraulichkeit (z.B. Verschlüsselungslösungen, Authentisierungsverfahren, Schutz vor äußeren Einflüssen etc.) - Integrität (z.B. Berechtigungskonzept, Prüfsummen, Plausibilitätskontrollen, Protokollierungskonzept etc.)	☐

- Verfügbarkeit (z.B. Redundanz von Hard- und Software sowie Infrastruktur, Datensicherungskonzept, Notfallstrategien, Vertretungsregelungen etc.) - Nichtverkettbarkeit (z.B. Berechtigungskonzept, Schnittstellenkontrolle, Identitätsmanagement etc.) - Transparenz (z.B. Verfahrensdokumentation, interne Kontrollen, Protokollierungskonzept) - Intervenierbarkeit (z.B. Prozessbeschreibung zur Sicherstellung von Betroffenenrechten des Datenschutzes) - Nachvollziehbarkeit und Nachprüfbarkeit, Vollständigkeit (z.B. Verfahrensbeschreibung, Freigabeverfahren, Erfassungskontrollen, Plausibilitätskontrollen) - Zeitgerechte Buchungen und Aufzeichnungen; zeitliche und sachliche Ordnung (z.B. Darstellbarkeit nach zeitlicher und nach sachlicher Ordnung, keine unprotokollierten Änderungen, Erfassungs-, Übertragungs- und Verarbeitungskontrollen) - Unveränderbarkeit bzw. Nachvollziehbarkeit von Änderungen (z.B. Sperrungen, Berechtigungskonzepte, Protokollierungen, Versionierungen) - Belegfunktion (z.B. Verfahrensbeschreibung, Freigabeverfahren, Autorisierung von Änderungen, Protokollierungen, Verknüpfungen und Vergabe von Zuordnungsmerkmalen) *Ein und dieselben Maßnahme kann mehreren Zielen gleichzeitig dienen.	
Interne Kontrollen (Bereiche und Tatbestände, Verfahren, Verantwortlichkeiten, Dokumentation)	☐
Verfahrensbeschreibung (s.o. unter II., Beschreibung von sachlogischer und programmtechnischer Lösung inklusive Änderungs- und Freigabeverfahren) (z.B. als Anlage 1)	☐
Arbeitsanweisungen für Anwender (z.B. Anlage 2)	☐
Berechtigungskonzept (Beschreibung aller Rechte und Rollen inklusive Administrationsrollen und technischer Benutzer und inklusive Beschreibung des Verfahrens zur Vergabe, zur Änderung und zum Entzug von Berechtigungen) (z.B. Anlage 3)	☐
Ordnungsmäßigkeitskonzept (Regelungen dazu, ob und inwieweit - zwei oder mehr Personen maßgeblich an einem einzelnen Geschäftsvorfall zu beteiligen sind, - nur eine Person den Geschäftsvorfall bearbeitet,	☐

- eine Anordnung zusätzlich von einer weiteren Person zu prüfen und freizugeben ist, - vollautomatisierte Verfahrensabläufe ohne Beteiligung einer Person Anwendung finden, - zusätzliche Prüfverfahren (Stichproben) einzusetzen sind und - Sicherungsmaßnahmen zu treffen sind.) (z.B. Anlage 4)	
Archivierungs- und Löschkonzept (Definition von Daten- und Dokumentenklassen mit den dazugehörigen Aufbewahrungsfristen, Beschreibung von Art und Umfang der Archivierung inklusive der zu archivierenden Angaben, Beschreibung des Löschverfahrens und der Verantwortlichkeiten) (z.B. Anlage 5)	☐
Protokollierungskonzept (z.B. Anlage 6)	☐
Inkrafttreten und Änderungsverfahren der DA	☐