Die Prüfdienste des Bundes
und der Länder informieren

Leitfaden

Elektronische Kommunikation
und
Digitalisierung in der Sozialversicherung

Version 6.2.1
Stand: 04.03.2026

Version:	Datum:	Grund d. Änderung:	Bearbeiter:
6.0	November 2021	Umfassende Überarbeitung der Version	AK E-Kommunikation
6.1	November 2023	Überarbeitung des Leitfadens Aktualisierung der Verlinkungen	AK E-Kommunikation und Digitalisierung in der Sozialversicherung (AK eKDig)
6.1.1	April 2024	Überarbeitung des Leitfadens	AK eKDig
6.2	April 2025	Überarbeitung des Leitfadens	AK eKDig
6.2.1	Mai 2026	Überarbeitung des Leitfadens	AK eKDig

Herausgeber:

ADV-Arbeitsgemeinschaft
Geschäftsstelle im Ministerium für Arbeit, Gesundheit und Soziales
des Landes Nordrhein-Westfalen
Fürstenwall 25
40219 Düsseldorf

Tel.: (0211) 855-4440
E-Mail: advag@mags.nrw.de

Bundesamt für Soziale Sicherung
Abteilung 6

Friedrich-Ebert-Allee 38
53113 Bonn

Ansprechpartner:
- Prüfgruppe IT des Referates 614 (Außenstelle Cloppenburg)
- Referat 611

E-Mail: LeitfadenEK@bas.bund.de

Wesentliche Änderungen zu Version 6.2

Neu aufgenommen

- Punkt 1.3.2.1 Art. 25 DSGVO
- Punkt 1.3.2.2 Art. 32 DSGVO
- Punkt 2.2.3 Verarbeitung von Sozialdaten zur Bestimmung individueller Gesundheitsrisiken (§ 25b SGB V)
- Punkt 2.2.4 Datenschutzkonforme Nutzung von Gesundheitsdaten
- Punkt 2.2.5 Nutzung von Daten zur Bekämpfung von Fehlverhalten im Gesundheitswesen
- Punkt 2.10.1 Data Act und Auftragsdatenverarbeitung
- Punkt 4.2.3.5 Eröffnung eines dauerhaften Online-Zugangs („Benutzer-Konto“)
- Punkt 5.3.4.1 Ersetzendes Scannen in der Sphäre der Krankenkasse
- Punkt 5.3.4.2 Ersetzende Scannen in der Sphäre der Leistungserbringer
- Punkt 7.3.1 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen
- Punkt 8.5.1 Speicherung von Informationen auf Endgeräten
- Punkt 8.5.2 Einwilligungsverordnung
- Punkt 8.5.3 Eingebundene Videos
- Punkt 9. Künstliche Intelligenz (KI)
- Punkt 9.1 Begriffsbestimmungen
- Punkt 9.1 Einsatz von KI
- Punkt 9.1 Fachliche Anforderungen an den Einsatz von KI

Änderungen / Ergänzungen

- Punkt 1.4.5 Anzeige an die Aufsicht jetzt unter Punkt 1.4.4
- Punkt 2.9 Gemeinsame Datenverarbeitung
- Punkt 4.2.3.2 Anforderungen an Authentifizierung
- Punkt 4.2.3.4 Gültigkeitsdauer einer Authentifizierung
- Punkt 4.2.3.6 jetzt 4.2.3.5
- Punkt 5.3 Zahlung
- Punkt 5.4 weggefallen bzw. s. unter neu aufgenommen Punkt 9 – 9.1
- Punkt 8.4.3 Digitale Identität / Gesundheits-ID

Inhalt:

0 Einleitung und Anwendungshinweise

Ziel dieses Leitfadens ist es, die gesetzlichen Vorgaben zur Digitalisierung aufzuzeigen und die hieraus abgeleiteten Anforderungen und Empfehlungen der Prüfdienste für die praktische Umsetzung zu formulieren. Dabei ersetzt der Leitfaden nicht die individuell durchzuführenden Risikoanalysen und das strukturierte Vorgehen bei der Auswahl, Einführung und (gesetzmäßigen) Umsetzung konkreter Maßnahmen.

Neben den durch Gesetze und Verordnungen festgelegten Rahmenbedingungen sind insbesondere die von den Bundesministerien herausgegebenen Richtlinien, Standards und Empfehlungen in den jeweils aktuellen Fassungen zu beachten.

Die Prüfdienste des Bundes und der Länder aktualisieren im Rahmen des Bund-Länder-Arbeitskreises Elektronische Kommunikation und Digitalisierung in der Sozialversicherung diesen Leitfaden regelmäßig hinsichtlich der rechtlichen Entwicklung auf europäischer und nationaler Ebene.

Den der Prüfung nach § 274 SGB V unterliegenden Institutionen wird empfohlen, ihre Verfahren entsprechend den Ausführungen in diesem Leitfaden zu gestalten. Die Institutionen werden im Text unter dem Begriff „**SV-Träger**“[1] zusammengefasst.

Es wird darauf hingewiesen, dass zur Vereinfachung der Lesbarkeit auf ein Gendering verzichtet wurde.

[1] **SV-Träger** i.S.v. § 274 SGB V: Krankenkassen, Pflegekassen, Arbeitsgemeinschaften, Landesverbände der Krankenkassen, GKV-Spitzenverband, Kassenärztliche Bundesvereinigung (KBV), Kassenzahnärztliche Bundesvereinigung (KZBV), Kassenärztliche Vereinigungen (KVs), Kassenzahnärztliche Vereinigungen (KZVs), Medizinischer Dienst des Spitzenverbandes Bund der Krankenkassen (MDS) Medizinische Dienste (MD).

1 Planung / Vorgehen / Gestaltung der Verfahren

1.1 Einleitung

Dieser Abschnitt bietet einen Überblick wichtiger Analysen, Maßnahmen und Rahmenbedingungen, die bei der Einführung oder Änderung von Verfahren aus dem Bereich der elektronischen Kommunikation durchzuführen oder zu beachten sind. Dabei ist es unerheblich, ob es sich um die Überarbeitung eines abgegrenzten, digitalen Informationsangebotes, die Erweiterung einer Online-Geschäftsstelle oder die Einführung eines Verfahrens zur automatisierten Sachbearbeitung handelt. Abhängig von Art, Umfang und Komplexität des Verfahrens kann die Durchführung einiger Schritte bzgl. des Detaillierungsgrades variieren. Die nachfolgend genannten Schritte tragen aus Sicht der Prüfdienste des Bundes und der Länder zum Projekterfolg und der Reduzierung von Risiken bei:

- Erstellung eines Projektvorschlages / Projektanbahnung,
- Vorbereitende Analysen und Maßnahmen,
  - Geschäftsprozessanalyse und -optimierung,
  - Datenschutzrechtliche Anforderungen an die Gestaltung von Verfahren,
  - Berücksichtigung von Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen),
  - Berücksichtigung von Art. 32 DSGVO (Sicherheit der Verarbeitung),
  - Berücksichtigung von Art. 35 DSGVO (Datenschutz-Folgenabschätzung),
  - Berücksichtigung von Art. 33 DSGVO (Einrichtung eines Meldewesens bei Datenschutzverletzungen),
- Begleitende und nachgehende Betrachtungen,
  - Zielerreichung,
  - Wirtschaftlichkeitsbetrachtung,
  - Risikomanagement / Compliance / Interne Kontrollsysteme,
  - Anzeigen an Aufsichtsbehörden,
  - IT-Sicherheit / Datensicherheit,
  - Change-Management,

Eine Geschäftsprozessanalyse und ggf. -optimierung, Analysen und Festlegungen zu Datenschutz und Datensicherheit, Wirtschaftlichkeitsbetrachtungen sowie – falls keine ausdrücklichen Ausnahmetatbestände vorliegen – die etwaige Anzeigepflicht an die Aufsichtsbehörde sind aus Sicht der Prüfdienste zwingend durchzuführen.
Da Änderungen oder Neueinführungen von Verfahren in Organisationen meist keine einmaligen Vorgänge sind, sollten die dabei durchzuführenden Schritte in einem Vorgehensmodell festgelegt sein. Ein solches Vorgehensmodell geht über die in diesem Abschnitt des Leitfadens dargestellten Punkte hinaus, da es auch wesentliche Rollen und deren Aufgaben, Meilensteine, Entscheidungspunkte sowie weitere Maßnahmen, Produkte und Dokumente beschreibt. Beispiele für sehr umfassende allgemeine Vorgehensmodelle sind das V-Modell XT, der Rational Unified Process oder hybride, agile Vorgehensmodelle; solche allgemeinen Modelle lassen sich häufig auf die jeweilige Organisation und Projektsituation zuschneiden (sog. Tailoring) oder können bei der Erstellung eines organisationsspezifischen Vorgehensmodells als Orientierung dienen.

Zur besseren Lesbarkeit wird beim Schutzbedarf auf die Kategorien des BSI-Standard 200_2 „normal“, „hoch“ und „sehr hoch“ Bezug genommen, ohne explizit auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit einzugehen. Dabei wird sich jeweils auf das höchste Schutzniveau der Schutzziele bezogen.
Für das Vertrauensniveau werden die drei Kategorien der eIDAS-Verordnung „niedrig“, „substantiell“ und „hoch“ verwendet.

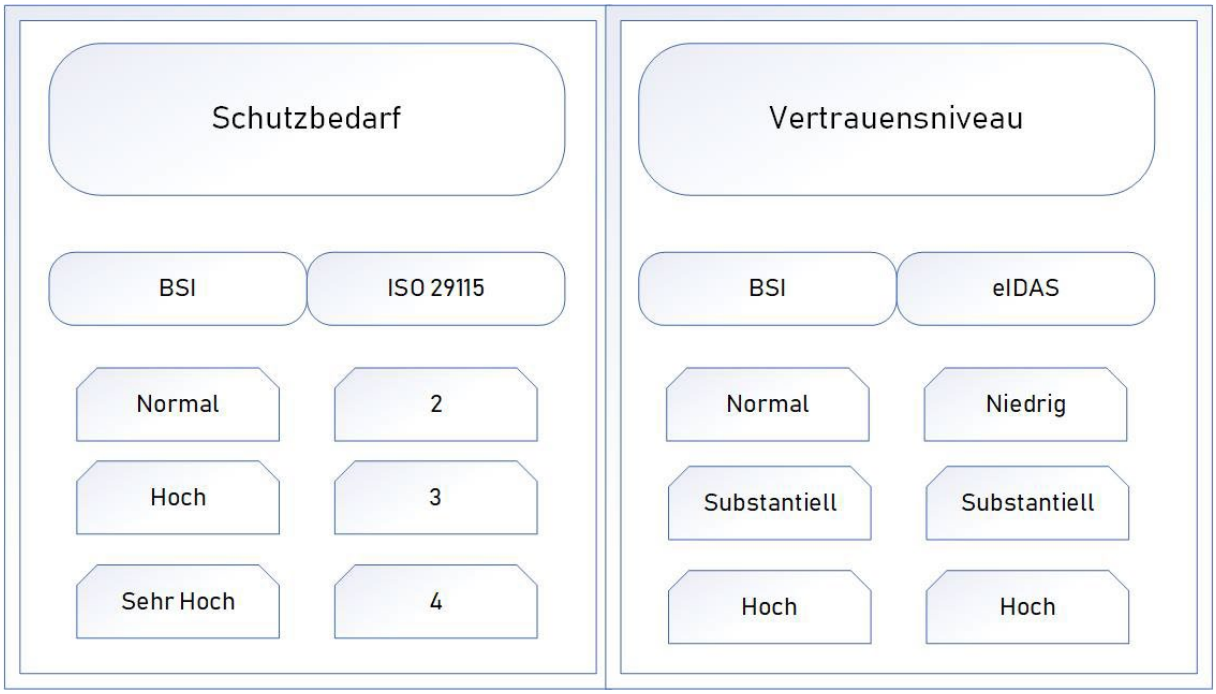

Abbildung 1 Schutzbedarf, Vertrauensniveau

1.2 Projektanbahnung

Zur Vorbereitung der Entscheidung, ob ein Projekt umgesetzt werden soll, sollte zunächst die aktuelle Situation im betroffenen Bereich betrachtet werden. Bei Änderungen oder der Ablösung bestehender Verfahren bzw. Prozesse sollten bestehende Prozessabläufe dargestellt und die wichtigsten Kennzahlen erhoben werden. In diesem frühen Stadium genügt eine grobe Darstellung der Prozessabläufe – eine detaillierte Geschäftsprozessanalyse erfolgt erst später im Projektverlauf. Weiterhin müssen die wesentlichen organisatorischen, technischen und rechtlichen Rahmenbedingungen identifiziert und beschrieben werden.

Durch die Analyse der Ausgangslage können ggf. vorhandene Schwächen ermittelt und bewertet werden. Sollten keine erheblichen Schwachstellen vorliegen und auch keine rechtlichen Vorgaben eine Änderung erforderlich machen, sollte bereits an dieser Stelle geprüft werden, ob das Projekt überhaupt notwendig ist.

Werden Schwächen identifiziert, bildet deren Behebung den Ausgangspunkt für die Formulierung konkreter Projektziele. Weitere Ansätze für die Projektziele können sich aus der Gesamtstrategie der Organisation oder deren IT- oder Digitalstrategie sowie aus der Umsetzung neuer rechtlicher Anforderungen ergeben. Grundsätzlich sollte nicht das neue Verfahren die Ziele bestimmen, sondern die Projektziele das Verfahren, anders ausgedrückt: es sollte nicht zuerst eine Softwarelösung ausgewählt werden, um danach die Einsatzmöglichkeit zu bestimmen.

Die Projektziele sollten so festgelegt und formuliert sein, dass ihre Erreichung messbar und prüfbar sind (Meilensteinplanung). Auch die Buchung der Projektkosten hängt von der jeweiligen Zielsetzung ab. Liegt die Zielsetzung eines Projektes im Bereich gesundheitlicher Aufklärung oder Mitgliederwerbung, sind die Kosten auch dann auf den entsprechenden Konten zu verbuchen, wenn für die Umsetzung des Projektes digitale Lösungen verwendet werden.

Unabhängig davon, ob die Projektziele aus der Gesamt- oder der Digital- / IT-Strategie hergeleitet wurden, sich aus Schwächen der bisherigen Prozesse oder aus rechtlichen Anforderun-

gen ergeben, sollte immer ein Abgleich mit den strategischen Zielen und Vorgaben vorgenommen werden. Einerseits sollte die Einführung oder Änderung eines Verfahrens zum Erreichen der strategischen Ziele beitragen, andererseits enthalten die übergeordneten Leitlinien Vorgaben, die berücksichtigt werden müssen. Eine Ausrichtung an der Gesamt- und IT-Strategie verringert auch das Risiko der Entstehung von Insellösungen, die sich schlecht in die bestehenden oder zukünftigen organisatorischen und technischen Strukturen einfügen.

Spätestens der Abgleich mit den Vorgaben aus den übergeordneten Leitlinien erfordert eine grobe Vorstellung von der organisatorischen und technischen Umsetzung des einzuführenden oder zu ändernden Verfahrens. Auch wenn die Ausgestaltung in dieser Phase i.d.R. noch nicht endgültig feststeht, sollte eine allgemeine Verfahrensbeschreibung erstellt werden. Davon ausgehend kann eine erste Einschätzung der zu erwartenden Risiken sowie der Wirtschaftlichkeit vorgenommen werden. Eine detaillierte Risikoanalyse sowie Wirtschaftlichkeitsbetrachtung erfolgen erst in den folgenden Projektphasen.

Schon in dieser frühen Phase sollte geprüft werden, ob Wechselwirkungen mit anderen Verfahren oder Geschäftsprozessen bestehen oder entstehen könnten. Andere betroffene Fachbereiche des SV-Trägers können so rechtzeitig informiert und beteiligt werden. Auf diese Weise lassen sich gegenläufige Entwicklungen vermeiden und mögliche Synergieeffekte nutzen. Im weiteren Projektverlauf wird dieser Punkt insbesondere im Zusammenhang mit Querschnitts- bzw. Basisfunktionen, Schnittstellen und Standards relevant.

Die Ergebnisse der oben beschriebenen Schritte sollten in Form eines Projektvorschlages festgehalten werden. Auf dieser Basis entscheiden die zuständigen Stellen, ob das Projekt begonnen werden soll. Ob eine vorgestellte Lösung umgesetzt wird, kann zu diesem Zeitpunkt noch nicht entschieden werden, da hierfür im Projekt zunächst die Entscheidungsgrundlagen zu erarbeiten sind.

Wurde beschlossen, dass ein Projekt begonnen werden soll, so müssen vor Beginn zahlreiche allgemeine Aufgaben des Projektmanagements durchgeführt werden. Dazu zählen u.a. die Bildung eines Lenkungsausschusses, die Ernennung einer Projektleitung, die Erstellung eines Projektplans sowie die Anmeldung und Sicherstellung der erforderlichen personellen, materiellen und finanziellen Ressourcen.

1.3 Vorbereitende Analysen und Maßnahmen

1.3.1 Geschäftsprozessanalyse und -optimierung

In den meisten Fällen stehen elektronische Verfahren nicht isoliert, sondern dienen dazu, Geschäftsprozesse zu unterstützen und zu optimieren. Sind die entsprechenden Prozesse nicht bereits in einem Prozesshandbuch beschrieben, so stellt die Analyse und Dokumentation bestehender bzw. die Konzeption neu einzuführender Geschäftsprozesse einen der wesentlichen Schritte bei der Einführung von Verfahren der elektronischen Kommunikation dar. Hieraus resultiert auch, dass es sich bei Projekten zur Einführung solcher Verfahren regelmäßig um Organisationsprojekte (inklusive fachlicher Fragen) und weniger um rein technische Projekte handelt.

In vielen Fällen bietet die Einführung elektronischer Verfahren neue Möglichkeiten zur Gestaltung der Prozesse (z. B. Parallelisierung, Automatisierung, medienbruchfreie Workflows). Von daher ist insbesondere bei bestehenden Geschäftsprozessen eine Analyse und Optimierung der Prozesse unter Berücksichtigung der ggf. neuen Möglichkeiten geboten. Dabei sollte der einzelne Geschäftsprozess nicht isoliert betrachtet werden, sondern immer im Zusammenhang mit seinen Vorgänger- und Nachfolgeprozessen, so dass Medienbrüche zwischen den Prozessen bzw. die Schaffung von „Insellösungen“ vermieden werden können – ggf. durch

Erweiterung des Einsatzbereichs des einzuführenden Verfahrens oder die Schaffung von Schnittstellen.

Neben den direkten Vorgänger- und Folgeprozessen sollten auch Wechselwirkungen mit weiteren Prozessen betrachtet werden. Abgesehen von ggf. ähnlich gestalteten Prozessen im selben oder in anderen Teilen der Organisation sind dabei auch die Wechselwirkungen zwischen Kern-, Management- und Unterstützungsprozessen zu berücksichtigen. Falls in der Organisation bereits eine Prozesslandkarte existiert, kann diese hierfür wichtige Anhaltspunkte bieten.

Bei der (Um-)Gestaltung von Prozessen sind neben fachlichen und technischen Anforderungen sowie den rechtlichen Rahmenbedingungen auch die organisationsweite Strategie sowie die IT-Strategie zu berücksichtigen.[2]

Für die strukturierte Darstellung von Geschäftsprozessen haben sich verschiedene grafische oder auch tabellarische Prozessmodelle etabliert. Einen Überblick bietet das Organisationshandbuch des Bundesverwaltungsamtes[3]. Innerhalb einer Organisation ist es in der Regel empfehlenswert, sich für eines dieser Modelle zu entscheiden und dieses möglichst organisationsweit zu verwenden. Hat sich das Prozessmodell in der Organisation etabliert, so erleichtert dies nicht nur die Dokumentation selbst, sondern vor allem auch den Umgang mit den Ergebnissen.

Trotz gründlicher Analyse und Konzeption kann sich im Wirk- / Produktivbetrieb zeigen, dass die neuen Prozesse die an sie gestellten Erwartungen nicht erfüllen oder die Prozesse nicht korrekt umgesetzt werden. Aus diesem Grund sollten die Prozesse nach einer festgelegten Anlaufphase nochmals kritisch betrachtet und ggf. angepasst werden.

1.3.2 Datenschutzrechtliche Anforderungen an Gestaltung von Verfahren

Bei der Gestaltung neuer bzw. der Änderung bestehender Verfahren sind Anforderungen zum Datenschutz zu beachten, die sich in diesem Leitfaden wiederfinden. Diese sind bereits frühzeitig in der Planung und Entwicklung zu berücksichtigen[4]

1.4 Begleitende und nachgehende Betrachtung

1.4.1 Zielerreichung

Die in der Vorphase gesetzten Ziele und deren Erreichungsfaktoren sind in der Umsetzungsphase fortzuschreiben und die Zielerreichung an den gesetzten Faktoren zu messen.

Begleitend und im Nachgang der Entwicklung sollten daher Maßnahmen vorgesehen werden, um die Zielerreichung zu messen.

---

[2] Zum eigenen Feld der strategischen Ansätze beim Einsatz von IT siehe die „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik“, Stand Mai 2025, abrufbar unter: https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/ver%C3%B6ffentlichungen_brh_lrh/it-mindestanforderungen.pdf?__blob=publicationFile&v=4

[3] Abrufbar unter: https://www.orghandbuch.de/Webs/OHB/DE/startseite/startseite-node.html

4 Abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM

Auf der Grundlage der Zielerreichung sind dann ggf. weitere Maßnahmen zu erörtern. Die Ergebnisse können dazu führen, dass bei der Umsetzung des Verfahrens / Geschäftsprozesses nachzusteuern ist, um die gesetzten Ziele (besser) zu erreichen.

Die Analyse der Zielerreichung kann auch als Erkenntnisquelle für die Weiterentwicklung bzw. die Entwicklung weiterer Prozesse herangezogen werden.
Dafür ist dann erforderlich, dass diese Erkenntnisse auch den beteiligten Bereichen bzw. Organisationseinheiten, die mit der Umsetzung weiterer Verfahren befasst sind, zur Verfügung gestellt werden.

Die Messung an den im Vorfeld festgelegten Zielerreichungsfaktoren, die ggf. vorzunehmende Anpassung der laufenden Projekte und die (permanente) Betrachtung und Weiterentwicklung der Prozesse, sollten fester Bestandteil des Aufbaus der Einführungsphase neuer Anwendungen / Prozesse und deren Erfolgskontrolle sein.

1.4.2 Wirtschaftlichkeitsbetrachtung

Vor einer Entscheidung über den Einsatz elektronischer Verfahren ist die Wirtschaftlichkeit des Gesamtverfahrens festzustellen (§§ 69 Abs. 2, 110a Abs. 2 SGB IV, vgl. EGovG). Hierfür sind die gängigen Verfahren zur Wirtschaftlichkeitsberechnung[5] (§ 69 Abs. 3 SGB IV) anzuwenden. Einzubeziehen sind auch Fragen zur Nachhaltigkeit und zu den Auswirkungen / Kosten bei einem Systemwechsel. Zu beachten ist hierbei, dass die Erfüllung gesetzlicher Vorgaben – insbesondere aus §§ 110a - c SGB IV sowie SGB X – Vorrang vor dem Gebot des wirtschaftlichen Handelns hat.

Die bereits in der Vorphase anzulegende grundlegende Wirtschaftlichkeitsbetrachtung ist im Verlauf des Umsetzungsverfahrens weiter fortzuschreiben.

Aus der Fortschreibung sollten regelmäßige Berichte mit Entwicklungen / entstehenden Risiken erstellt werden.

Nach Abschluss der Implementierung sollte die abschließende Wirtschaftlichkeitsbetrachtung analysiert werden, um Anhaltspunkte / Annahmen für weitere Verfahren zu erhalten bzw. dort Risiken frühzeitig erkennen zu können.

Es wird empfohlen, im Rahmen einer Evaluation des neu eingeführten Verfahrens zu überprüfen, inwieweit die Prognosen eingetreten sind, die der Wirtschaftlichkeitsbetrachtung zugrunde lagen.

1.4.3 Informationen zur Bewertung von Risikomanagement

Das (bestehende) Risikomanagement des SV-Trägers muss auch die neuen Systeme und Prozesse umfassen.

Daher sind aus dem Umsetzungsprozess bzw. der Entwicklung heraus die entsprechenden Informationen aus dem konkreten Verfahren für das Risikomanagement aufzubereiten und diesem bzw. der hierfür zuständigen Stelle zuzuleiten.

[5] Band 18 der Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung BWV (Präsident des Bundesrechnungshofes): „Anforderungen an Wirtschaftlichkeitsuntersuchungen finanzwirksamer Maßnahmen nach § 7 Bundeshaushaltsordnung“.

Die identifizierten Risiken (z. B. Datenverlust / Datensicherheit, eingeschränkte Erreichbarkeit, technische Fehler, IT-Sicherheit / Ausfall, Ausschluss fachliche Fehler, Cyberangriffe) sollten monetär wie nicht-monetär bewertet und dokumentiert werden.

Maßnahmen zu deren Bewältigung sind zu entwickeln und auch noch im Wirkbetrieb fortzuschreiben sowie regelmäßig zu überprüfen und anzupassen.

Anhaltspunkte für eine derartige Risikoanalyse bietet der BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz.

Ein gesondertes Augenmerk bei der Einführung und Umsetzung neuer Systeme und Prozesse ist auch auf die Einhaltung weiterer gesetzlicher, vertraglicher und sonstiger Vorgaben (wie interner Richtlinien) zu setzen, deren Einhaltung durch das Compliance-System der Träger betrachtet werden soll. Insbesondere sind bei IT-gestützten Verfahren die entsprechenden datenschutzrechtlichen Vorschriften (siehe Punkt 2.), die Vermeidung einer unzulässigen Weitergabe von Informationen, ausreichende Authentifizierungsverfahren und Ausschluss der unbeabsichtigten Weitergabe von Informationen sicherzuzustellen. Daher sollten die neuen Instrumente auch im Hinblick auf das (bestehende) Compliance-Umfeld der SV-Träger ausgerichtet werden und eine entsprechende Information an die verantwortliche Stelle erfolgen.[6]

1.4.4 Anzeige an Aufsichtsbehörden

Vor Einführung des Verfahrens sind die gesetzlich vorgesehenen Meldungen/Anzeigen an die zuständige Aufsichtsbehörde zu übermitteln.

Gem. § 85 Abs. 3b Nr. 2 SGB IV ist dabei (bereits) die Absicht, sich zur Aufgabenerfüllung an Einrichtungen im Sinne dieses Gesetzbuches zu beteiligen (d.h. eine Einrichtung zu gründen oder zu erwerben, sich an einer Einrichtung zu beteiligen oder eine Beteiligung an einer Einrichtung zu erhöhen) anzuzeigen. Gleiches gilt nach § 85 Abs. 3b Nr. 1 SGB IV für die Absicht, Datenverarbeitungsanlagen und -systeme anzukaufen, zu leasen oder anzumieten oder sich an solchen zu beteiligen und der Aufsichtsbehörde vor Abschluss verbindlicher Vereinbarungen anzuzeigen. Dies gilt auch für die Beschaffung von Datenverarbeitungsprogrammen. Jede Anzeige hat so umfassend und rechtzeitig zu erfolgen, dass der Aufsichtsbehörde vor Vertragsabschluss ausreichend Zeit zur Prüfung und Beratung des Versicherungsträgers bleibt.

Bei der Einführung von E-Government-Verfahren, elektronischer Vorgangsbearbeitungssysteme oder der elektronischen Langzeitspeicherung handelt es sich in der Regel um grundlegende Maßnahmen im DV-Bereich. Diese sind somit rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht anzuzeigen.
Die Aufsichtsbehörden haben den „Grundleitfaden 85“[7] erstellt. Dieser bildet den Rahmen für die Anzeige und die Wirtschaftlichkeitsbetrachtung und ist demnach zu beachten.
Soweit sich der Versicherungsträger bei der Erfüllung seiner gesetzlich vorgeschriebenen Aufgaben zulässigerweise eines Dritten bedient, kann er nach Anzeige bei der Aufsichtsbehörde auch die damit notwendigerweise verbundenen Aufgaben des Rechnungswesens durch diesen Dritten wahrnehmen lassen (§ 19 SVRV).

Die Aufsichtsbehörde im Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg hat die Grundsätze für Anzeigen bezüglich Datenverarbeitungsanlagen und –systemen sowie

[6] Zum Aufbau eines Compliance Managements siehe Bundesamt für Sicherheit in der Informationstechnik ORP.5: Compliance Management (Anforderungsmanagement) in der jeweils gültigen Fassung.

[7] Abrufbar unter: https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/grundleitfaden-85-fuer-anzeigen-zur-beschaffung-bzw-entwicklung-von-datenverarbeitungsanlagen-und-systemen-sowie-programmen-nach-85-abs-1-saetze-2-bis-6-sgb-iv/

Datenverarbeitungsprogrammen gemäß § 85 Abs. 3 b SGB IV sowie bezüglich der Verarbeitung von Sozialdaten im Auftrag gemäß § 80 SGB X (Grundsätze 85 und 80 IT) aktualisiert.[8]

1.4.5 IT-Sicherheit / Datensicherheit

Eine auf den bestehenden und beschriebenen Geschäftsprozessen sowie den ermittelten Risiken basierende Gesamtdarstellung der Informationssicherheit sollte für den Träger aufgebaut und fortgeschrieben werden. Anhaltspunkte bietet hierfür insbesondere der BSI-Standard 200-1.

Die BSI-KRITIS-Verordnung bestimmt den Anwendungsbereich in der gesetzlichen Sozialversicherung. Mit dem NIS-2-Umsetzungsgesetz (NIS2UmsuCG) am 06.12.2025, dass das BSIG novelliert, werden Betreiber kritischer Anlagen (KRITIS) automatisch als „besonders wichtige Einrichtungen“ eingestuft. Dies erweitert die bestehenden Pflichten um umfassende Risikomanagementmaßnahmen, Registrierungspflichten beim BSI sowie eine dreistufige Meldepflicht für erhebliche Sicherheitsvorfälle. Der Sektor Sozialversicherung wurde zudem aus dem Finanzsektor herausgelöst und steht nun eigenständig. Betreiber kritischer Anlagen sind nach § 39 Abs.1 BSIG gesetzlich verpflichtet, alle drei Jahre gegenüber dem BSI nachzuweisen, dass ihre IT-Sicherheit auf dem aktuellen Stand der Technik ist. Diese Nachweise enthalten eine Einschätzung der prüfenden Stelle zur Wirksamkeit der Managementsysteme für Informationssicherheit (ISMS) und Geschäftskontinuität (Business Continuity Management System, BCMS) beim geprüften Betreiber.

Bei Auslagerung von IT-Dienstleistungen verbleibt die Sicherheitsverantwortung auch beim KRITIS-Betreiber. Betreiber kritischer Anlagen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen.

Darüber hinaus legt der Gesetzgeber in § 392 SGB V und § 103a SGB XI spezifische Anforderungen an die IT-Sicherheit fest, die nicht nur für Betreiber kritischer Anlagen gelten, sondern für alle Kranken- und Pflegekassen im Regelungsbereich verbindlich sind. Hiernach sind Kranken- und Pflegekassen verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Kranken- und Pflegekasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind - insbesondere angesichts der hohen Bedrohungslage im Gesundheitssektor. Die NIS2-Richtlinie verstärkt diese Pflichten durch erweiterte Anforderungen an Risikoanalysen, Supply-Chain-Sicherheit und Führungsverantwortung, wobei der B3S-GKV/SV weiterhin als geeignete Maßnahme zur Erfüllung dient. Gemäß § 217f Abs. 4c SGB V legt der GKV-SV den branchenspezifischen Sicherheitsstandard im Sinne des § 392 Abs. 4 SGB V und § 103a Abs. 3 SGB XI in der jeweils aktuellen Fassung als Richtlinie für die Krankenkassen verbindlich fest.

Gemäß § 217f Abs. 4c SGB V und § 103a Abs. 8 SGB XI berichtet der GKV-SV jährlich dem BMG und den Kassenaufsichten über den Umsetzungsstand des branchenspezifischen Sicherheitsstandards bei den einzelnen Kassen sowie die ergriffenen Maßnahmen).

[8] Abrufbar unter https://sozialministerium.baden-wuerttemberg.de/de/soziales/sozialversicherung/aufsicht-im-bereich-sozialversicherung/

1.4.6 Interne Kontrollsysteme

Die neuen bzw. geänderten Anwendungen sind durch die hierfür zuständigen Stellen in das interne Kontrollsystem des SV-Trägers einzubeziehen.

Dabei sind insbesondere folgende Punkte vorzunehmen:

- Aufnahme in einer Verfahrensübersicht und in einem Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO),
- Prüfung der Anwendungen auf Einhaltung der allgemeinen Vorgaben des Risikomanagements / der Compliance,
- Einbezug der Umsetzung / des Wirkbetriebs der Anwendungen im Prüfplan der verantwortlichen Stellen.

1.4.7 Change-Management

Änderungen von Prozessen bergen vielfältige Risiken. Zum Teil sind es solche, die auch beim (Neu-)Aufbau von Prozessen auftreten. Änderungen bergen aber auch spezifische Risiken, wie z. B. mögliche Eingriffe in laufende Systeme bzw. Migration von Daten, die im Rahmen von Änderungsprozessen und der Umsetzungsplanung angemessen zu berücksichtigen sind.

Daher sollten die Geschäftsprozesse zum Change-Management zur Änderung von Prozessen, Anwendungen sowie fachlicher und technischer Parameter allgemein festgelegt werden. In die Änderungsverfahren sollten auch jeweils die verantwortlichen Stellen des SV-Trägers nach einem festen Geschäftsprozess verpflichtend eingebunden werden:

- Fachbereich (materielles Recht und Fachprozesse)
- IT-Bereich
  Allen Anwendungen und Technologien ist eigen, dass diese nicht als zeitlich befristetes „Projekt“ gedacht werden sollten, sondern in längeren „Lebenszyklen“ zu sehen sind mit den entsprechenden dauerhaften Aufwänden für
  - den erforderlich strukturierten Aufbau,
  - die Entwicklung von Prototypen,
  - eine ggf. differenzierte Testphase,
  - die eigentliche Umsetzung,
  - die Klärung neu auftretender rechtlicher Fragen bei Weiterentwicklung,
  - die stetige Überprüfung der Ergebnisse, der Weiterentwicklung und des Trainings,
- Datenschutz,
- IT-Sicherheit,
- Risikomanagement und Internes Kontrollsystem,
- Speicherung und Archivierung.

Eine nachvollziehbare Dokumentation des Änderungsprozesses ist dringend zu empfehlen.

1.5 Umsetzung der eIDAS-Verordnung

Die eIDAS-Verordnung[9] legt einen einheitlichen Rechtsrahmen für den elektronischen Identitätsnachweis und für Vertrauensdienste (z. B. elektronische Signaturen, Siegel und Zeitstempel) fest. Die Umsetzung der Verordnung in deutsches Recht erfolgt durch das Vertrauensdienstegesetz (VDG).[10]

Am 20. Mai 2024 trat die Novellierung der eIDAS-Verordnung, kurz eIDAS 2.0, in Kraft. Sie setzt neue Ziele und Anforderungen für die elektronische Identifizierung und Vertrauensdienste. Ein zentrales Element ist die Einführung einer europäischen digitalen Identität (EUDI), die den Bürgern und Unternehmen eine sichere Identifizierung online und offline sowie die Nutzung von Authentifizierungsdiensten in der gesamten EU ermöglicht.
Die Instrumente der Verordnung sind bei der Gestaltung der Authentifizierungs-/ Identifikationskonzepte der SV-Träger im Rahmen der elektronischen Kommunikation in die Überlegungen einzubeziehen (siehe § 36a Abs. 2a Nr. 3 Buchst. a SGB I).

Organisationszertifikate
Die Bedeutung der Organisationszertifikate, deren Anwendung im deutschen Recht durch § 17 VDG geregelt wird, liegt in der Wirkung als Herkunftsnachweis. Das Zertifikat stellt keinen Ersatz der persönlichen Unterschrift dar, kann aber den Nachweis der Authentizität (auch bei Bescheiden) erbringen. Technisch entsprechen die Zertifikate einer elektronischen Signatur, sind aber „nur“ einer juristischen Person zugeordnet.

Dadurch wird ein organisationsweiter bzw. steuerbarer (nach Funktion, Bevollmächtigung, Berechtigung) Einsatz möglich, ohne dass – wie bei der elektronischen Signatur – Zertifikate für Mitarbeitende der juristischen Person erforderlich sind.

Fernsignaturen
Fernsignaturen, die im VDG nicht geregelt sind, so dass die Bestimmungen der eIDAS-Verordnung nach Ansicht der Prüfdienste herangezogen werden können, beinhalten die Möglichkeit der Verwendung einer qualifizierten elektronischen Signatur (QES) ohne Smartcard / Lesegeräte.
Dadurch kann eine Authentifizierung auf hohem Niveau und gleichzeitig eine Nutzbarkeit für mobile Dienste erreicht werden (siehe Punkt 3.2.2, Abbildung 3).

1.6 Betrieb eines Hinweisgebersystems

Das Hinweisgeberschutzgesetz (HinSchG) sieht die Verpflichtung zu einem Hinweisgebersystem vor. Dieses System muss wiederum entsprechend der unter Punkt 1. des Leitfadens erörterten allgemeinen Anforderungen an Verfahren des Trägers ausgestaltet sein.

Meldekanäle können intern von hierfür benannten Personen oder Abteilungen betrieben oder extern durch Dritte bereitgestellt werden. Eine organisatorische Zuordnung kann z. B. an die Personal-, Rechts- oder Compliance-Abteilung oder die Interne Revision oder an den Datenschutz erfolgen, sofern Interessenskonflikte ausgeschlossen sind.

Zulässigkeit der Datenverarbeitung
Das HinSchG als nationale Umsetzungsnorm der Richtlinie (EU) 2019/1937 (Whistleblowing-Richtlinie (WBRL), insbesondere Art. 8) fungiert für verpflichtete Unternehmen als Ermächti-

[9] Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-Verordnung/eidas-verordnung_node.html
[10] Gesetz vom 18. Juli 2017, BGBl. 2017 I, S. 2745.

gungsgrundlage im Sinne des Art. 6 Abs. 1 S. 1 Buchst. c DSGVO für die Verarbeitung personenbezogener Daten im Hinweisgebersystem. Unternehmen mit weniger als 50 Beschäftigten fallen nicht in den Anwendungsbereich des nationalen Rechts zur Umsetzung der WBRL. Bei einer Interessenabwägung gem. Art. 6 Abs. 1 S. 1 Buchst. f DSGVO wird der Abschluss einer Vereinbarung nach Art. 88 DSGVO empfohlen.

Das Datenschutzkonzept für das Hinweisgebersystem sollte sich auf die Minimierung der datenschutzrechtlichen Risiken für die Rechte und Freiheiten der betroffenen Personen (Löschkonzept, Unterrichtungs- und Auskunftspflichten, Beschränkung von Zugriffsrechten, Datenminimierung) fokussieren.

Eine DSFA ist vor Einführung eines Meldekanals zwingend durchzuführen. Verwiesen wird auf die Orientierungshilfe der Datenschutzkonferenz aus dem Jahr 2018.[11]

[11] Siehe Orientierungshilfe der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf

2 Datenschutz

2.1 Einleitung

Datenschutz ist Grundrechtsschutz und schützt das Recht des Bürgers auf informationelle Selbstbestimmung. Er unterliegt dem Rechtsprinzip des Verbotes mit Erlaubnisvorbehalt. Daher ist das Sammeln von Daten (auch für die SVT) grundsätzlich verboten, es sei denn es liegt eine Erlaubnis vor. Diese Erlaubnis kann durch Rechtsnormen oder Einwilligung erfolgen und führt also zwangsläufig zu einer Beschränkung der Befugnisse der vom Amtsermittlungsprinzip verpflichteten SV-Träger.

Datenschutz wirkt präventiv. Wenn Daten an Unbefugte abfließen, ist der Schaden eingetreten. Ein Verstoß gegen das Verbot der Erhebung von personenbezogenen Daten stellt eine rechtswidrige Handlung dar. Für den erforderlichen Personenbezug gem. Art. 4 Nr. 1 DSGVO genügt es, dass ein unmittelbarer Bezug zur Person des Betroffenen herstellbar ist.

Das Prinzip der Rechtmäßigkeit der Datenverarbeitung (Art. 5 DSGVO) verlangt das Bestehen einer Rechtsgrundlage für die Datenverarbeitung, dies bezieht sich auf das „Ob“, und „Wie“ der Datenverarbeitung. Die Verarbeitung besonderer Kategorien personenbezogener Daten - hierzu zählen auch Gesundheitsdaten - ist grundsätzlich verboten, Art. 9 Abs. 2 DSGVO nennt demgegenüber verschiedene Ausnahmetatbestände. Die in § 67 Abs. 2 S. 1 SGB X definierten Sozialdaten bilden eine eigene abschließend geregelte (§ 35 Abs. 2 SGB I) spezifische Datenkategorie nach deutschem Recht. Es handelt sich um personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB verarbeitet werden.

2.2 Grundlagen

2.2.1 Die Einwilligung als Rechtsgrundlage zur Datenverarbeitung

Die Einwilligung als Rechtsgrundlage ist nur dann einzuholen, wenn keine gesetzliche Verarbeitungsbefugnis besteht. Sie setzt ein aktives Verhalten –eine „Willensbekundung“ - voraus und verlangt die Opt-In-Lösung.

Gesundheits-, biometrische und genetische Daten, die zugleich Sozialdaten sind, dürfen nach wie vor nur bei Vorliegen einer Einwilligung oder einer normativen Ermächtigung im SGB (Art. 9 Abs. 4 DSGVO i. V. m. § 67a bzw. § 67b Abs. 1 SGB X) verarbeitet werden.

Die Prüfdienste empfehlen, ein Einwilligungsmanagement aufzusetzen, das sich auf alle technischen (z. B. Cookies) und fachlichen Anwendungsfälle (z. B. Kontaktaufnahme) bezieht. Wichtige Hinweise hierzu enthält die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder herausgegebenen Orientierungshilfe der Aufsichtsbehörden für Anbieter von digitalen Diensten (OH Digitale Dienste).

2.2.2 Verarbeitung von Sozialdaten zu Forschungszwecken

Wenn nach § 75 SGB X Sozialdaten für ein bestimmtes Vorhaben an einen Dritten übermittelt werden sollen, ist im Regelfall die Einholung einer Einwilligungserklärung erforderlich, die nachfolgende Mindestinhalte enthalten muss:[12]

[12] Abrufbar unter: https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20250709_FAQ___75.pdf

- Erläuterung des Vorhabens und der Evaluation,
- Vollständige Erläuterung worin genau der Versicherte einwilligt,
- In dem Fall, dass die Einwilligung zusammen mit anderen Einwilligungen wie z. B. einer Teilnahme an einer besonderen Versorgung eingeholt werden soll, getrennte Einwilligungsmöglichkeiten und optische Trennung,
- Erläuterung des Zwecks der Übermittlung, Verweis auf § 75 SGB X,
- Aufzählung der betroffenen Daten,
- Benennung aller Datenempfänger (auch der Vertrauensstelle),
- Hinweis auf die Freiwilligkeit der Einwilligung,
- Auflistung der Betroffenenrechte,
- Aufklärung über die Widerrufsmöglichkeiten.

2.2.3 Verarbeitung von Sozialdaten zur Bestimmung individueller Gesundheitsrisiken (§ 25b SGB V)

§ 25b SGB V regelt die datengestützte Erkennung individueller Gesundheitsrisiken durch die gesetzlichen Krankenkassen und ist mit dem Gesundheitsdatennutzungsgesetz vom 22.03.2024 in Kraft getreten.

Versicherte müssen vorab transparent über die Verarbeitung informiert und auf ihr Widerspruchsrecht hingewiesen werden. Die Krankenkassen dürfen keine Daten aus der elektronischen Patientenakte (ePA) für diese Zwecke nutzen. Erkannte Risiken werden den betroffenen Versicherten schriftlich in verständlicher Sprache mitgeteilt, ergänzt um Handlungsempfehlungen und eine Begründung. Diese Hinweise werden zusätzlich in der ePA gespeichert, sofern die betroffene Person eine ePA nutzt.
Die Datenverarbeitung darf nur auf Basis bereits vorliegender Abrechnungsdaten erfolgen; neue Daten dürfen nicht erhoben werden. Krankenkassen müssen geplante Auswertungen bei ihrer Aufsichtsbehörde anzeigen und den Verwaltungsrat darüber informieren.[13]

2.2.4 Datenschutzkonforme Nutzung von Gesundheitsdaten

Der Europäische Gesundheitsdatenraum (EHDS) schafft wichtige Voraussetzungen für die Weiterentwicklung der Gesundheitsversorgung in Deutschland und Europa. Die EHDS-Verordnung ist am 26. März 2025 in Kraft getreten. Mit ihr wurde ein EU-weiter Rechtsanspruch auf einen schnellen und einfachen Zugang zu den eigenen elektronischen Gesundheitsdaten für Patientinnen und Patienten geschaffen. Auch Angehörige der Gesundheitsberufe sollen einen umfassenden Zugang zu Daten erhalten, die für die optimale Behandlung von Patientinnen und Patienten notwendig sind (Primärnutzung). Die EHDS-Verordnung legt zudem die weitere Nutzung von Gesundheitsdaten (Sekundärnutzung) fest: Es werden die Voraussetzungen für die datenschutzkonforme Nutzung von Gesundheitsdaten geregelt.
Die elektronische Patientenakte (ePA s. Kapitel 9) – wie im Rahmen des Digital-Gesetzes (DigiG) und des Gesundheitsdatennutzungsgesetzes (GDNG) geregelt – eignet sich auch im Kontext der EHDS als zentraler Zugangspunkt für Patientinnen und Patienten genauso wie für Leistungserbringer. Die Entscheidung über eine Datennutzung und Datenweitergabe in der Versorgung wird auch unter den Vorgaben der EHDS-Verordnung durch die Patientinnen und Patienten getroffen. Das Widerspruchsrecht gegen die Sekundärnutzung ist für die Daten aus

[13] Abrufbar unter:
https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20250522_Rundschreiben___25bSGBV_FAQ.pdf
https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20250522_FAQ___25bSGBV.pdf

der ePA bereits im GDNG angelegt: Über die ePA werden Gesundheitsdaten für die Sekundärnutzung datenschutzkonform bereitgestellt, wenn die Versicherten dieser Nutzung nicht widersprechen (Opt-Out).

Das Gesundheitsdatennutzungsgesetz (GDNG) ist am 26. März 2024 in Kraft getreten und regelt die erleichterte Nutzbarkeit von Gesundheitsdaten für gemeinwohlorientierte Zwecke. Gemäß § 2 Nr. 1 GDNG sind Gesundheitsdaten Daten im Sinne des Art. 4 Nr. 15 DSGVO. Solche Gesundheitsdaten können zugleich Sozialdaten nach § 67 SGB X sein.
Beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) wird eine zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten im Sinne von § 3 Abs. 1 GDNG eingerichtet, diese soll Datennutzende beim Zugang zu Gesundheitsdaten unterstützen und beraten und hat folgende Aufgaben (§ 3 Abs. 2 GDNG):

- Bereitstellen eines öffentlichen Metadaten-Katalogs,
- Beraten bei der Identifizierung und bei der Lokalisierung der benötigten Gesundheitsdaten,
- Unterstützen bei Anträgen auf Zugang zu den Daten bei den datenhaltenden Stellen,
- Informieren der Öffentlichkeit über die eigenen Aktivitäten,
- Führen eines öffentlichen Antragsregisters mit Informationen zu gestellten Anträgen, zu den Nutzern der Daten sowie zu den Vorhaben und deren Ergebnissen,
- Erstellen von Konzepten zum Datenschutz und zur Datensicherheit sowie zur Verknüpfung und gemeinsamen Verarbeitung von pseudonymisierten Gesundheitsdaten verschiedener datenhaltender Stellen.

Zu den datenhaltenden Stellen gemäß § 2 Nr. 3 GDNG gehören insbesondere gesetzlich geregelte datenhaltende Stellen wie das Forschungsdatenzentrum Gesundheit nach § 303d SGB V und die Plattform nach § 64e Abs. 9 SGB V. Datennutzende sind Stellen nach § 2 Nr. 4 GDNG.

Werden auf der Grundlage des GDNG Gesundheitsdaten ohne Einwilligung der betroffenen Personen zu Forschungszwecken verarbeitet, sind die für das Forschungsvorhaben Verantwortlichen verpflichtet, vor Beginn der Datenverarbeitung das Forschungsvorhaben in einem anerkannten Primärregister für klinische Studien zu registrieren (Registrierungspflicht), sofern dieses die Registrierung gestattet.

Bei bestehender Registrierungspflicht, sind die für das Forschungsvorhaben Verantwortlichen außerdem verpflichtet, die Forschungsergebnisse innerhalb von 24 Monaten nach Abschluss des Forschungsvorhabens in anonymisierter Form und in einer für die Allgemeinheit zugänglichen Weise zu veröffentlichen (Publikationspflicht).

2.2.5 Nutzung von Daten zur Bekämpfung von Fehlverhalten im Gesundheitswesen

Personenbezogene Daten, die von den Stellen nach § 197a Abs. 1 SGB V und § 81 a Abs. 1 SGB V zur Erfüllung ihrer Aufgaben erhoben wurden, dürfen zur Bekämpfung von Fehlverhalten im Gesundheitswesen verwendet werden.

2.3 Rechte der Betroffenen

Die Rechte betroffener Personen (Art. 12 - 23 DSGVO), deren Daten verarbeitet werden, bringen für Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO Pflichten mit sich. Die Etablierung

eines praktikablen Verfahrens, um DSGVO-konform auf Ansprüche der Betroffenen reagieren zu können, ist empfehlenswert.[14]

Die Rechte der betroffenen Personen sind ergänzend im SGB X geregelt. Diese Rechte sind bei der Gestaltung von Verfahren durch den SV-Träger zu berücksichtigen. Im Einzelnen betrifft dies folgende Rechte:

- Informationspflichten bei der Erhebung von Sozialdaten bei der betroffenen Person gem. § 82 SGB X,
- Informationspflichten bei der Erhebung von Sozialdaten nicht bei der betroffenen Person gem. § 82a SGB X,
- Auskunftsrecht der Betroffenen gem. § 83 SGB X,
- Recht auf Berichtigung und Löschung gem. § 84 SGB X.[15]

2.4 Datenschutzerklärung

Generell muss in der Datenschutzerklärung über jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgeklärt werden (Art. 13 DSGVO).

Eine Datenschutzerklärung muss Antwort auf folgende Fragen geben können:

- Welche personenbezogenen Daten werden erhoben?
- Was passiert mit den erhobenen Daten?
- Warum werden überhaupt Daten erhoben?
- Findet eine gemeinsame Datenverarbeitung gem. Art. 26 DSGVO statt?
- Werden die erhobenen Daten an Dritte weitergegeben?
- Findet ein grenzüberschreitender Datenverkehr statt?
- Welche Maßnahmen werden zur Gewährleistung der Sicherheit der Daten ergriffen?

Außerdem gehört in eine Datenschutzerklärung die:

- Nennung der Rechtsgrundlage,
- Information über Art und Umfang der Datenerhebung,
- Separater Hinweis auf das Widerrufsrecht des Nutzers,
- Rechte des Nutzers.

Arten der Datenerhebung
Abhängig von der Art des erbrachten Dienstes und des Umfangs der erhobenen Daten empfiehlt sich aus Gründen der Verständlichkeit eine Untergliederung der Datenschutzerklärung. In einer kurzen Einleitung kann über Sinn und Zweck der Datenschutzerklärung informiert sowie die datenschutzrechtlich verantwortliche Stelle – grundsätzlich der Webseitenbetreiber – genannt werden. Darüber hinaus bietet sich eine Auflistung der verschiedenen Arten von Datensätzen und eingesetzten Tools an, zum Beispiel:

a) IP-Adresse,
b) Browser-Daten,
c) Cookies,
d) Analyse-Tools,

[14] Abrufbar unter: https://www.datenschutz-bayern.de/infothek/OH_Gemeinsame_Verantwortlichkeit.pdf

[15] Zum Verhältnis Berichtigung von Diagnosedaten gem. § 84 SGB X vor dem Hintergrund des Korrekturverbotes gem. § 303 SGB V siehe 92. Arbeitstagung der Aufsichtsbehörden der SV-Träger, TOP 16.

e) Social Plugins,
f) Sonstige Daten.

Die DSGVO-Checkliste zur Datenschutzerklärung (nach Art. 13 DSGVO) sieht folgendes vor:

Zwingend:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch Vertreter),
- Zweck und Rechtsgrundlage der Verarbeitung,
- Falls Rechtsgrundlage der Art. 6 Abs. 1 Buchst. f) DSGVO ist: Angabe der berechtigten Interessen des Verantwortlichen oder Dritten,
- Aufklärung über Rechte des Betroffenen (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragung),
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde,
- Speicherdauer der Daten (jedenfalls die Kriterien für die Festlegung dieser Dauer).

Optional bzw. situationsabhängig:

- Falls eine Einwilligung Rechtsgrundlage ist: Hinweis auf die Möglichkeit des jederzeitigen Widerrufs,
- Sofern vorhanden: Kontaktdaten des Datenschutzbeauftragten,
- Bei gesetzlicher oder vertraglicher Pflicht zur Datenerhebung: Aufklärung des Betroffenen über diese Pflicht und die möglichen Folgen einer Nichtbereitstellung,
- Beim Einsatz automatisierter Entscheidungsfindungen (einschl. Profiling): Aufklärung hierüber, insbesondere die zugrundeliegende Logik, die Tragweite und die angestrebten Auswirkungen für den Betroffenen.

Im Falle der Beteiligung Dritter:

- Bei einer Weitergabe an Dritte: Angabe der Empfänger / Kategorie von Empfängern,
- Angabe der Absicht zur Datenübermittlung ins Ausland (dann auch Angabe des von der Kommission festgelegten Datenschutzniveaus des jeweiligen Drittlandes).

Im Falle von Übermittlungen nach Art. 46, 47 oder 49 DSGVO: Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

2.5 Geeignete technische und organisatorische Maßnahmen (TOM)

Die DSGVO verpflichtet nach Art. 24 DSGVO Verantwortliche dazu, geeignete technische und organisatorische Maßnahmen (TOM) zu implementieren, um gemäß Art. 25 Abs. 1 DSGVO die Datenschutzgrundsätze wie Datenminimierung (Art. 5 Abs. 1 Buchst. c)) und Datensicherheit (Art. 5 Abs. 1 Buchst. f)) sicherzustellen. Diese Maßnahmen sind an den Stand der Technik, die Eintrittswahrscheinlichkeit und Schwere möglicher Risiken sowie die Implementierungskosten anzupassen. (Datenschutz durch Technik, auch "privacy by design" genannt.) Wirtschaftliche Argumente dürfen keine unzureichenden Schutzmaßnahmen rechtfertigen.
Das Gesetz nennt in Art. 32 Abs. 1 DSGVO als wichtige, aber nicht abschließende Vorgaben für Maßnahmen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Hierbei handelt es sich zum einen um IT-Sicherheitskonzepte wie etwa einen geeigneten Virenschutz, eine ausreichende Stromversorgung oder ein Backup-Programm. Auch organisatorische Maßnahmen wie etwa eine wirksame Zutritts-, Zugangs- und Zugriffskontrolle zählen dazu. Zur internen Sicherheit gehören auch Dienstanweisungen an die Beschäftigten – etwa eine Richtlinie zur Kontrolle der Weitergabe von Daten, ein Archivierungs-, Aufbewahrungs- und Löschkonzept, eine Anweisung, wie auf Auskunftsbegehren der Betroffenen zu reagieren ist oder was zu tun ist, wenn ein Notfall eintritt.

Technische Geräte und vor allem IT-Anwendungen müssen so voreingestellt werden, dass nur solche Daten erhoben werden, die erforderlich sind, um den jeweiligen bestimmten Verarbeitungszweck zu erreichen (Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DSGVO, auch „privacy by default“ genannt).

Die Verpflichtung zur Umsetzung technischer und organisatorischer Maßnahmen (TOM) nach § 392 Abs. 1 SGB V und § 103a Abs. 1 SGB XI wird von den Kranken- und Pflegekassen durch die Anwendung des jeweils gültigen branchenspezifischen Sicherheitsstandards erfüllt (vgl. hierzu Punkt 1.4.5).

2.6 Datenschutz-Folgenabschätzung (DSFA)

Für die DSFA gem. Art. 35 DSGVO müssen Verantwortliche einschätzen, ob die jeweilige Verarbeitung voraussichtlich hohe Risiken für die Rechte oder Freiheiten des Betroffenen ausweist. Sie erfolgt in bis zu drei Stufen und ist schriftlich zu dokumentieren.

1. Eine systematische Risikobewertung (Schwellwertanalyse) ist vorzunehmen. Hier müssen alle einzelnen Prozesse daraufhin überprüft werden, ob im Einzelfall voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlichem Risiko reicht eine gemeinsame Abschätzung (Art. 35 Abs. 1 S. 2 DSGVO). Ein solches Risiko besteht nach Art. 35 Abs. 3 DSGVO insbesondere bei der Verwendung neuer Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten. Auch kann aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein solches Risiko bestehen. Schließlich kann die Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten oder Religionszugehörigkeit i. S. d. Art. 9 DSGVO) eine weitere Prüfung notwendig machen. Als weitere Hilfestellung für die Einschätzung dienen die ersten Leitlinien zur DSFA der Art. 29-Datenschutzgruppe[16]. Die Aufsichtsbehörden gem. Art. 35 Abs. 4 DSGVO veröffentlichen eine Liste[17] von Verarbeitungsvorgängen, für die eine DSFA verbindlich durchzuführen ist.

2. Wenn ein solches Risiko im Hinblick auf den Prozess besteht, muss in einer zweiten Stufe eine Bewertung dahingehend vorgenommen werden, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten. Der Nachweis zur Einhaltung der DSGVO muss erbracht werden.

[16] Abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
[17] Abrufbar unter: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html

3. Verbleibt trotz des Eingreifens technischer und organisatorischer Maßnahmen ein hohes Risiko für die Rechte und Freiheiten der natürlichen Person muss in einer dritten Stufe die zuständige Datenschutzaufsichtsbehörde konsultiert werden (Art. 36 Abs. 1 DSGVO).

Diese kann dann innerhalb von acht Wochen Empfehlungen aussprechen (Art. 36 Abs. 2 DSGVO). Diese Frist kann je nach Komplexität der geplanten Verarbeitung von personenbezogenen Daten von der Aufsichtsbehörde verlängert werden.

Eine Datenschutz-Folgenabschätzung ist vor Aufnahme der Verarbeitungsvorgänge durchzuführen[18]. Im Einzelfall können verschiedene TOMs dazu beitragen, die gesetzlichen Anforderungen (vgl. Art. 5, 24, 25, 32 DS-GVO und § 22 Abs. 2 BDSG) zu erfüllen.

Die Datenschutzbeauftragten des SV-Trägers sind beratend in die Durchführung einer DSFA einzubinden (Art. 35 Abs. 2 und Art. 39 Abs. 1 c DSGVO).

2.7 Melde- und Informationspflichten bei Datenpannen

Nach Art. 33 DSGVO müssen grundsätzlich alle Verletzungen des Schutzes personenbezogener Daten gemeldet[19] werden, es sei denn, das Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich. Verantwortliche müssen sowohl den zuständigen Datenschutzaufsichtsbehörden[20] unverzüglich, möglichst binnen 72 Stunden, nach Bekanntwerden der Verletzung gem. Art. 33 Abs. 3 DSGVO die erforderlichen Informationen übermitteln. Die betroffene Person ist persönlich über die Verletzung zu benachrichtigen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 Abs. 1 DSGVO).

Ist eine der Bedingungen nach Art. 34 Abs. 3 DSGVO erfüllt, ist eine Benachrichtigung der betroffenen Person nicht erforderlich.

2.8 Verzeichnis der Verarbeitungstätigkeiten

In Art. 30 DSGVO ist vorgeschrieben, dass der Verantwortliche bzw. der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten“[21] führen müssen. Ähnlich dem bisherigen Verfahrensverzeichnis handelt es sich dabei um eine Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden. Die neue Verordnung sieht im Vergleich zur bisherigen Rechtslage zusätzliche Angaben vor, wie z. B. Name und Kontaktdaten des ggf. bestellten Datenschutzbeauftragten, Löschfristen und die TOM. Mustervordrucke und Ausfüllhinweise sind auf den einschlägigen Datenschutzportalen des Bundes und der Länder zu finden. Das Verzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

2.9 Gemeinsame Datenverarbeitung

Nach Art. 26 DSGVO legen die gemeinsam Verantwortlichen die Zwecke der und die Mittel zur Verarbeitung fest. Die gemeinsam Verantwortlichen vereinbaren in transparenter Form, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht und wer welchen Informationspflichten

[18] DSK-Konferenz vom 06.11.2023, S. 6 f.
[19] Abrufbar unter https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-186ef7dce1/
[20] Datenschutzbehörden und Rechts- bzw. Fachaufsicht der SV-Träger.
[21] Abrufbar unter: https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

gemäß den Art. 13 und 14 DSGVO nachkommt. Es wird als ausreichend erachtet, diese Informationen auf einer Webseite bereitzustellen. Ungeachtet der in der Vereinbarung erfolgten Aufteilung, können betroffene Personen ihre Rechte stets bei und gegenüber jedem der gemeinsam Verantwortlichen ausüben (Art. 26 Abs. 3 DSGVO).

Gemeinsam verantwortliche öffentliche Stellen dürfen und müssen bei Nichtvorliegen entsprechender gesetzlicher Ausgestaltungen eine Vereinbarung abschließen. Beispielhaft ist für die gesetzliche Aufgabenverteilung nach Art. 26 Abs. 1 S. 2 DSGVO der § 307 Abs. 5 S. 2 und 3 SGB V betreffend die Aufgabe der gematik, eine koordinierende Stelle einzurichten.

Jeder der gemeinsam Verantwortlichen haftet nach Art. 82 Abs. 4 i. V. m. Abs. 2 . 1 DSGVO im Falle rechtswidriger Verarbeitung für den gesamten Schaden, sofern er nicht sein fehlendes Verschulden nachweisen kann (Art. 82 Abs. 3 DSGVO). Hat ein Verantwortlicher den gesamten Schaden beglichen, ist ein Schadensersatz im Innenverhältnis auf der Grundlage von Art. 82 Abs. 5 DSGVO möglich. Daher ist eine dezidiert ausgearbeitete Vereinbarung, die die jeweiligen Verantwortlichkeiten genau abgrenzt, unerlässlich, um evtl. Schadensersatzansprüche im Innenverhältnis durchsetzen zu können.

Die Schwierigkeit[22] in der Praxis besteht in der Abgrenzung zwischen Auftragsverarbeitung – bei der der Auftraggeber immer verantwortliche Stelle ist – und einer gemeinsamen Verantwortlichkeit. Diese ist immer dann anzunehmen, wenn ein tatsächlicher Einfluss auf die wesentlichen Elemente der Verarbeitung besteht. Dies heißt jedoch nicht, dass jeder der Beteiligten eine umfassende Kontrolle über alle Umstände und Phasen der Verarbeitung haben muss; die verschiedenen Beteiligten an der Datenverarbeitung können in verschieden Phasen und in unterschiedlichem Ausmaß einbezogen sein.

Zur Abgrenzung können folgende Fragestellungen dienen:

Wer entscheidet darüber,

- welche Daten verarbeitet werden,
- wie lange sie aufzubewahren bzw. wann zu löschen sind,
- wer Zugriff hat,
- für welche Zwecke die Daten verarbeitet werden.

Auch die Frage, ob sich der Zweck der Datenverarbeitung ohne den oder die anderen Beteiligten erreichen lässt, kann zur Klärung beitragen.

2.10 Auftragsverarbeitung

Die SV-Träger schließen als Verantwortliche einen Vertrag mit dem Auftragsverarbeiter[23] gemäß § 80 SGB X i. V. m. Art. 28 DSGVO.

Die Auftragsverarbeitung darf aufgrund der spezialrechtlichen Regelung des § 80 SGB X nur im Inland, in einem EU- oder EWR-Mitgliedsstaat oder in einem Drittstaat, für den ein Angemessenheitsbeschluss nach Art. 45 VO (EU) 2016/679 vorliegt, erfolgen (siehe Punkt 7.5). Eine Verarbeitung ist auch dann möglich, wenn mit dem Auftragsnehmer verbindliche Schutzmaßnahmen (Artikel 32 DSGVO i. V. m. Erwägungsgrund 83) vereinbart werden, die ein Abfließen der Sozialdaten ins Ausland unmöglich machen. Wesentlich ist hierbei der physische

[22] Abrufbar unter: https://www.datenschutz-bayern.de/infothek/OH_Gemeinsame_Verantwortlichkeit.pdf
[23] Beachte Besonderheit K(7)V'en, bei der die empfangenen k(Z)v Verantwortliche für die ihnen zugesandten Daten wird (§ 77 Abs. 6 SGB V)

Ort der Datenverarbeitung, nicht nur der Sitz oder die Niederlassung des Auftragsverarbeiters. Neben den nach Art. 28 DSGVO gestellten Anforderungen an die Auftragsverarbeitung, zählen insbesondere der Gegenstand und die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten beider Vertragspartner wie bspw. die technischen und organisatorischen Maßnahmen, das Datenschutzkonzept und die Überwachung, die Erteilung von Unterauftragsverhältnissen zu den Vertragsinhalten. Die zutreffenden vertraglichen Regelungen und Anforderungen an den Auftragsverarbeiter nach Art. 28 Abs. 3 DSGVO sind schriftlich zu vereinbaren.

Mit der Anzeige des Auftrages des Verantwortlichen (§ 80 Abs. 1 S. 1 SGB X) an die Aufsichtsbehörde besteht die Verpflichtung folgende Auskünfte zu erteilen:

- Kontaktdaten zum Auftragsverarbeiter,
- vorhandene technische und organisatorische Maßnahmen zur Sicherstellung des Sozialdatenschutzes,
- Information über zu verarbeitende Daten,
- Information über Kreis der betroffenen Personen,
- Untervertragsverhältnisse.

Diese Anzeige, die insbesondere auch die Gründe zur Auftragsverarbeitung enthalten muss, ist vom Verantwortlichen rechtzeitig zu stellen, damit seitens der Aufsichtsbehörde noch vor Auftragserteilung genügend Zeit besteht, durch Beratung und gegebenenfalls sonst zur Verfügung stehenden Aufsichtsmitteln intervenieren zu können. Es besteht jedoch keine Genehmigungspflicht. Handelt es sich bei der Auftragsverarbeitung um eine öffentliche Stelle, so hat auch diese Stelle – wie der Verantwortliche selbst - eine Anzeige an die zuständige Aufsichtsbehörde zu richten (§ 80 Abs. 1 S. 2 SGB X).
Der Auftragsbearbeiter ist nach den getroffenen vertraglichen Regelungen (Art. 28 Abs. 1 S. 1 DSGVO) des verantwortlichen Auftraggebers weisungsgebunden und zur Unterstützung des Verantwortlichen verpflichtet (§ 80 Abs. 1 SGB X i. V. m. Art. 28 Abs. 3 DSGVO). Er hat eine Meldepflicht bei datenschutzrechtlichen Verstößen gegenüber dem Verantwortlichen (siehe auch Punkt 2.7). Er sollte für seine umgesetzten Aktivitäten eine eigene Dokumentation führen, um auch seiner Verantwortlichkeit im Sinne des Art. 28 Abs. 10 DSGVO nachvollziehbar festzuhalten (siehe auch Punkt 2.8). Dem Verantwortlichen obliegt die Verpflichtung, seiner Kontrollfunktion umfänglich nachzukommen (Art. 24 DSGVO). Diese ist zwingend vertraglich zu vereinbaren.

Der Vertrag zur Auftragsverarbeitung kann unter zur Hilfenahme der „Checkliste zur Prüfung AVV“ und dazu ergangenen Hinweisen „Hinweisen zur Nutzung der Checkliste Prüfung AVV“ formell und inhaltlich nachvollzogen werden[24].

2.10.1 Data Act und Auftragsverarbeitung

Ein Großteil der Verpflichtungen aus dem Data Act (Datenverordnung-DVO) kommt ab dem 12. September 2025 zur Anwendung und damit u. a. für Anbieter vernetzter Produkte und verbundener Dienste die Pflicht, bestimmten Akteuren Zugang zu Daten und deren Nutzung zu gewähren. Hiervon sind auch personenbezogene Daten betroffen, denn der Data Act findet auf beide Datenarten Anwendung (Art. 1 Abs. 2 DVO). Es bestehen Wechselwirkungen zwischen DVO und DSGVO, die zu beachten sind. Kommen Auftragsverarbeiter auch im Anwendungsbereich des Data Act zum Einsatz, sind besondere Vorkehrungen zu treffen:

[24] Abrufbar unter: https://www.datenschutz-berlin.de/pressemitteilung/pruefung-von-auftragsverarbeitungsvertraegen-von-web-hostern/

Auftragsverarbeiter sind zwar selbst nicht als Dateninhaber zu qualifizieren (ErwG 22 S. 4 DVO, ErwG 29 S. 2 DVO) diese sollen aber sicherstellen, dass Zugangsverlangen von Auftragsverarbeitern entgegengenommen und bearbeitet werden. Es empfiehlt es sich, die Verträge (Art. 28 DSGVO, § 80 SGB X) um entsprechende Weisungsbefugnisse zu ergänzen.

Um im Vorfeld die Weichen für eine datenschutzkonforme Umsetzung des Data Act zu stellen, werden folgende Maßnahmen beispielhaft benannt:

- Prüfung der Datenklassifizierungen;
- Prüfung und ggf. Anpassung der Verantwortlichkeiten, um festzustellen, wer für welche Verarbeitung als datenschutzrechtlich „Verantwortlicher“ und somit als Dateninhaber nach dem Data Act zu qualifizieren ist;
- Prüfung und Anpassung des Datennutzungskonzepts (einschließlich des Sperr- und Löschkonzepts und des Zugriffskonzepts) angesichts der über die DSGVO-Vorgaben hinausgehenden Anforderungen an Zweckbindung, Löschung etc.;
- Ergänzung der Datenschutzerklärungen um diejenigen berechtigten Interessen, auf die ggf. Datenweitergaben und andere -verarbeitungen nach dem Data Act gestützt werden;
- Anpassung von Einwilligungen und Nutzungsverträgen zur Verankerung rechtfertigungsbedürftiger, vom Data Act ausgelöster Datenverarbeitungen;
- Prüfung und Ergänzung sowohl von Auftragsverarbeitungsverträgen als auch von Verträgen über gemeinsame Verantwortlichkeit, um angemessene Weisungen bzw. Vereinbarungen zur Ermöglichung von Datenzugangsgewährungen zu integrieren. Ggf. sind die Verträge um ein Sonderkündigungsrecht für den Fall sich ändernder rechtlicher Gegebenheiten im Drittland zu ergänzen.

2.11 Datenschutzmanagement

Ergänzend zu den dargelegten Ausführungen empfehlen wir das Standard-Datenschutzmodell (SDM)[25] der deutschen Datenschutzaufsichtsbehörden. Hierbei handelt es sich um eine Methode, mit der die Übereinstimmung von Anforderungen des Datenschutzrechts und technisch-organisatorischen Funktionen personenbezogener Verfahren überprüfbar werden. Es unterstützt die Transformation abstrakter rechtlicher Anforderungen in konkrete technische und organisatorische Maßnahmen.[26]

Die rechtlichen Anforderungen der Datenschutz-Grundverordnung werden vom SDM vollständig erfasst, mit Hilfe von Gewährleistungszielen systematisiert und über die Gewährleistungsziele in von der Verordnung geforderte technische und organisatorische Maßnahmen überführt.
Das SDM benennt konkret sieben Gewährleistungsziele des Datenschutzes, welche für die Anwendung des SDM von elementarer Bedeutung sind. Im Einzelnen sind dies:

- Datenminimierung,
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz und

[25] Abrufbar unter: https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html
[26] Abrufbar unter: https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20180522_RdSchr_DSGVO_DSMS.pdf

- Intervenierbarkeit.

Das im SDM beschriebene Datenschutzmanagement führt Verantwortliche durch alle Phasen der Verarbeitung personenbezogener Daten und ermöglicht somit die kontinuierliche Aufrechterhaltung einer rechtssicheren Verarbeitung.

3 Übertragung von Papierunterlagen in elektronische Form

3.1 Allgemeines

Dieser Abschnitt des Leitfadens beschreibt das Scanverfahren, also die Überführung von Papierdokumenten in die elektronische Form. Die nachfolgenden Empfehlungen beziehen sich hauptsächlich auf folgende Themen:

- Klassifizierung von Papierdokumenten
- Dokumentation des Scan-Vorgangs
- Sicherungsmaßnahmen und
- Vernichtung der Originalbelege

Ziel dieses Abschnittes ist es, die gesetzlichen Vorgaben zu dieser Thematik zusammenzutragen und die hieraus abgeleiteten Anforderungen der Prüfdienste für die praktische Umsetzung zu formulieren. Die Anforderungen und Empfehlungen betreffen neu entwickelte und zukünftig realisierte Scanprojekte.

Dieser Leitfaden ersetzt nicht die individuellen Risikoanalysen und das strukturierte Vorgehen bei der Auswahl, Einführung und (gesetzesmäßigen) Umsetzung konkreter Maßnahmen. Folgende Gesetze und Verordnungen sind für das Scanverfahren von besonderer Bedeutung:

- §§ 35 und 36a SGB I,
- §§ 110a bis 110c SGB IV,
- §§ 284 ff. SGB V,
- §§ 67 ff. SGB X,
- §§ 6 und 7 des Gesetzes zur Förderung der elektronischen Verwaltung (EGovG),
- Vertrauensdienstegesetz (VDG),
- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG,
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO),
- Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (SVRV),
- Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV).

Des Weiteren sind folgende, vom Bundesamt für Sicherheit in der Informationstechnik (BSI), des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und vom Bundesinnenministerium herausgegebenen Werke, Standards und Empfehlungen in den jeweils aktuellen Fassungen zu beachten:

- BSI-Standards 200-1, 200-2, 200-3 und 100-4,
- IT-Grundschutzkompendium,
- Technische Richtlinie TR-03138 „Ersetzendes Scannen“ (TR-RESISCAN),
- Technische Richtlinie TR-03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ (TR-ESOR),
- Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer B3S-GKV/PV.

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

3.2 Übertragung in die elektronische Form

Das Übertragen von Papierdokumenten in die elektronische Form ist in § 110a SGB IV geregelt. Dieser Paragraph gilt als spezialrechtliche Norm vorrangig gegenüber der in § 7 EGovG enthaltenen Regelung. Ergänzend enthält das EGovG Hinweise darauf, wie das Scanverfahren technisch und organisatorisch auszugestalten ist, nämlich nach dem „Stand der Technik". Dieser kann sich z. B. aus Richtlinien des BSI ableiten.

Die TR-RESISCAN beschreibt die technischen und organisatorischen Anforderungen für Scanprozesse und Scanprodukte, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Ziel der TR ist es, den Anwendern in Wirtschaft und Verwaltung einen Handlungsleitfaden und eine Entscheidungshilfe zum ersetzenden Scannen zu geben. Im Hinblick auf die Informationssicherheit werden die bei einem Scanprozess bedeutsamen Bedrohungen in einer Strukturanalyse für alle Datenobjekte und Kommunikationsbeziehungen systematisch dargestellt. Auf Grundlage einer darauf aufbauenden Schutzbedarfsanalyse und anhand der entlang der verschiedenen Scanphasen durchgeführten Risikoanalyse werden konkrete Sicherheitsmaßnahmen beschrieben.

Die TR enthält einen modularen Anforderungskatalog, der unterschiedliche Sicherheitsstufen umfasst. Während es in der „Basisstufe" vor allem um einen grundsätzlichen ordnungsgemäßen und mit grundlegenden Sicherheitsmaßnahmen ausgestalteten Scanprozess geht, werden in den „Ausbaustufen" besondere Anforderungen an Integrität, Verfügbarkeit und Vertraulichkeit mit entsprechend erhöhten Sicherheitsmaßnahmen beschrieben.

Die nachfolgend aufgeführten Anforderungen an den Scanprozess leiten sich grundsätzlich aus dieser Richtlinie ab.

Die Prüfdienste des Bundes und der Länder werden die sich aus diesem Leitfaden sowie der TR-RESISCAN ergebenden Anforderungen bei Prüfungen als Prüf- und Bewertungsgrundlage heranziehen.

3.2.1 Scannen von Papierdokumenten

§ 110a SGB IV regelt, wie mit Papierdokumenten zu verfahren ist, die gescannt werden sollen. Diese sind durch ein maschinelles Scanverfahren in elektronische Dokumente zu übertragen. Hierbei sind folgende Besonderheiten zu beachten:

3.2.1.1 Klassifizierung der Papierdokumente

Der SV-Träger hat für die einzuscannenden Dokumente eine fachliche Schutzbedarfsanalyse zu erstellen, in der hinsichtlich der Schutzziele „Integrität", „Vertraulichkeit" und „Verfügbarkeit" eine Klassifizierung vorzunehmen ist. Die TR-RESISCAN schlägt hier eine dreistufige Aufteilung in „Normal", „Hoch" und „Sehr Hoch" vor.

Während für ein als „Normal" klassifiziertes Dokument einfache technisch-organisatorische Schutzmaßnahmen im Scanprozess implementiert werden müssen, fordert die TR für „Hoch" und „Sehr Hoch" eingestufte Dokumente die Anwendung kryptographischer Sicherungsmittel.

Für den SV-Träger bedeutet dies, dass er unterschiedliche technisch-organisatorische Verfahren für jede Dokumentenklasse einführen müsste. Aufgrund des hohen Aufwandes erscheint eine solche Lösung nicht wirtschaftlich.

Die Prüfdienste empfehlen daher, das Scanverfahren so zu gestalten, als seien nur Dokumente mit Schutzbedarf „Sehr Hoch“ zu scannen. Nähere Ausführungen zu den Anforderungen an ein solches Scanverfahren sind der TR-RESISCAN und ihren Anhängen zu entnehmen.

3.2.1.2 Bildliche und inhaltliche Übereinstimmung

Die Wiedergabe auf einem Bildträger oder die Daten auf einem anderen dauerhaften Datenträger müssen mit der dieser zu Grunde gelegten schriftlichen Unterlage bildlich und inhaltlich vollständig übereinstimmen. Die Gesetzesbegründung führt dazu aus, dass die „Wiedergabe bei einem späteren Abruf einen vollständigen „urschrift-getreuen“ Ausdruck oder eine sonstige entsprechende Reproduktion garantiert“. Daraus könnte nunmehr abgeleitet werden, dass ausschließlich eine Farbabbildung mit qualifizierter elektronischer Signatur urkundliche Beweiskraft besitzt.

Die Prüfdienste des Bundes und der Länder sind der Auffassung, dass die SV-Träger aus Gründen der Rechtssicherheit alle papiergebundenen Dokumente in Farbe einscannen sollten. Lediglich bei Vordrucken, bei denen Farbe keine Beweiskraft besitzt, sondern nur als Ausfüllhilfe für die spätere Texterkennung dient (z. B. AU-Bescheinigungen, Verordnungen), ist ein Farb-Scan entbehrlich. Für die Prüfung von RSA-relevanten Belegen (z. B. Verordnungen) wird die Vorlage von Graustufen-Images mit allen Formatierungszeichen für ausreichend erachtet.

Es muss sichergestellt sein, dass die Belege urschriftgetreu gescannt werden.

Die Anbringung eines elektronischen Eingangsstempels bzw. einer automatischen Paginierung ist unmittelbar vor dem Scanvorgang zulässig. Nach dem Scanvorgang (auf dem Image) automatisch angebrachte elektronische Eingangsstempel sind nicht zulässig, da das Image dann kein originalgetreues Abbild des Urbeleges mehr ist. Dabei muss der elektronische Eingangsstempel dem tatsächlichen Eingangsdatum des Papierdokumentes entsprechen.

Es ist sicherzustellen, dass eingehende Schriftstücke, bei denen es sich offensichtlich um unbeglaubigte Kopien oder Papier-Faxe handelt, nicht automatisch gescannt und signiert werden. Vielmehr ist hier erforderlich, diese Schriftstücke vor dem Signiervorgang mit einem Stempelaufdruck „Kopie“ bzw. „FAX“ zu versehen.

3.2.1.3 Dokumentation des Scan-Vorgangs

Gemäß TR 03138 (TR-RESISCAN) ist festzuhalten, wer ein Dokument in die elektronische Form übertragen hat (Transfervermerk).
Die gescannten Images sind vom Scan-Operator bzw. der Sachbearbeitung zu signieren. Hierdurch wird bestätigt, dass das Original vorlag und in die elektronische Form übertragen wurde.

Nach Art. 5 Abs. 1 Buchst. f DSGVO sind Daten gegen Schädigungen durch geeignete technische und organisatorische Maßnahmen zu schützen.
Es wird empfohlen, alle einzuscannenden Papierdokumente mit dem Schutzbedarf „Sehr Hoch“ („Hoch“ nach eIDAS-VO) zu klassifizieren und die daraus resultierenden Anforderungen gem. TR-RESISCAN umzusetzen (siehe auch Punkt 3.2.1.1). Hierzu gehört u.a.

- der Einsatz kryptographischer Sicherungsmittel, wie der qualifizierten elektronischen Signatur (QES) oder eines elektronischen Siegels und
- die Protokollierung, wer das Scansystem wann und in welcher Weise genutzt hat.

Letzteres kann über einen Transfervermerk sichergestellt werden, der neben dem Ersteller des Scanproduktes auch Informationen über Zeitpunkt der Erfassung sowie Ergebnis der Qualitätssicherung beinhaltet. Der Transfervermerk muss mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden (vgl. TR-RESISCAN).

Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte zu verhindern, müssen daher geeignete Mechanismen für den Schutz der Integrität dieser Datenobjekte (Scanprodukt, Transfervermerk) eingesetzt werden (siehe auch Abschnitt 4, Punkt 4.3.2; weiterführend TR-RESISCAN).

3.2.2 Formen der Signatur

Einzelplatzsignatur:
Klassischer Einsatzbereich ist der Sachbearbeiter-Arbeitsplatz (SB-Platz), an dem einzelne Dateien elektronisch signiert und versendet werden sollen. Die Einzelplatzsignatur erfordert grundsätzlich, dass sich die hierzu benötigte Hardware (Kartenlesegerät) und Software (Signatursoftware) im direkten Zugriffsbereich des Anwenders befindet. Im Übrigen gelten hier dieselben Sicherheitsvorschriften, die auch bei sonstigen SB-Plätzen – gem. Dienstanweisung – zu beachten sind.

Stapelsignatur:
Beim Stapelsignaturverfahren werden große Mengen Beleggutes gescannt. Die erzeugten Images werden mit Hilfe einer Signaturanwendungskomponente an einen Scan- / Signaturarbeitsplatz übertragen, an dem der Signaturvorgang initiiert werden kann.

Vorteil dieses Verfahrens gegenüber dem der Einzelsignatur liegt im Zeitgewinn: Einscannen, Signieren und Speichern von Papierbelegen können im Stapelbetrieb erfolgen. Dies erfordert, den Übernahmeprozess effizient zu gestalten. Hier entsteht ein Problem, wenn deshalb der vollständige Übernahmeprozess bestehend aus

- Scannen des Dokuments,
- Erstellen der Bilddatei und
- Signieren der Datei

automatisiert wird, so dass nicht davon ausgegangen werden kann, dass der Bediener jedes Dokument vor dem Signieren visuell auf Übereinstimmung prüft; ein mögliches Schadensrisiko ist durch technische und organisatorische Vorkehrungen zu minimieren

Vor der Signierung ist die Gesamtheit der eingescannten Dokumente auf ihre Richtigkeit (Vollständigkeit, Lesbarkeit, Unversehrtheit, etc.) zu prüfen Die Prüfdienste empfehlen, unter Berücksichtigung von § 7 EGovG, dass der Signiervorgang grundsätzlich zeitlich und räumlich in unmittelbarem Zusammenhang mit dem Einscannen erfolgt. Die Signatur sollte hierbei von der Person angebracht werden, die das Dokument auch in die elektronische Form überführt hat („Stapelsignatur“).

Alternativ dazu besteht die Möglichkeit, die Images unmittelbar nach deren Herstellung durch einen anderen als den Scan-Operator signieren zu lassen.

Fernsignatur:
Die eIDAS-2.0 bietet die Möglichkeit der Fernsignatur. Hierbei wird eine qualifizierte elektronische Signatur nicht mehr mit einer Signaturkarte erstellt, sondern von einem qualifizierten Vertrauensdienstanbieter im Auftrag des Sozialversicherungsträgers.

Die beauftragende Organisation muss gegenüber dem Vertrauensdienstanbieter ihre Identität nachweisen und über eine gesicherte Verbindung zu kommunizieren.

Die Integrität des zu signierenden Dokuments wird mittels eines kryptografisch sicheren Prüfwerts (Hash) erbracht. Dieser Hashwert wird über das zu signierende Dokument in das Protokoll der Online-Ausweisfunktion eingebunden. Auf diesem Wege kann kryptografisch nachweisbar sichergestellt werden, dass sowohl auf Seiten des Nutzers als auch des Vertrauensdienstanbieters das identische, zu signierende Dokument vorgelegen hat.

Für Revisionszwecke müssen die einzelnen Schritte der Scanverarbeitung nachvollziehbar sein. Zur Qualitätssicherung gehören die unter Punkt 3.2.1.3 „Dokumentation des Scan-Vorgangs“ aufgeführten Maßnahmen; unter anderem der Transfervermerk (wer hat wann das Dokument gescannt) oder die Bestätigung der Übereinstimmung zwischen Scan und Original.

Elektronische Siegel:
Wird die Signatur mittels eines elektronischen Siegels nach der eIDAS-VO erstellt, ist sicherzustellen, dass das Scanprodukt die sichere Netzwerkumgebung nicht verlässt (vgl. 3.2.3 Sicherheitsmaßnahmen). Die sichere Signaturerstellungseinheit (SSEE) zählt dabei nicht zu den für das Scannen eingesetzten IT-Systemen und kann somit auch außerhalb des sicheren Netzwerkbereiches vorgehalten werden. In diesem Fall kann ein Verlassen des Scanproduktes dadurch umgangen werden, dass lediglich der digitale Hashwert des Scanproduktes an den zentralen Siegelserver übermittelt und dort -signiert wird. Die anschließend zurückgegebene Signatur ist innerhalb der „sicheren Umgebung“ in bzw. an das Scanprodukt einzubauen.

3.2.3 Sicherheitsmaßnahmen

Bei Verfahren zur Übertragung von Papierunterlagen in die elektronische Form (Scan- / Signaturverfahren) sind Sicherheitsmaßnahmen erforderlich.

Das Einscannen und Signieren geringer Papiermengen kann unter der Voraussetzung, dass eine Einzelsignatur an jedem Dokument angebracht wird, auch an den normalen Arbeitsplätzen erfolgen. Nachfolgend gehen wir insbesondere auf die Besonderheiten des Stapelsignaturverfahrens ein.

Bauliche und technische Vorkehrungen:
Der Einsatz von Stapelsignaturverfahren sollte in einer abgesicherten Umgebung erfolgen.

Die Signaturanwendungskomponenten sind derart zu konfigurieren, dass die Signaturerstellungseinheit lediglich für die Signatur eines Stapels freigeschaltet wird; die Stapelgröße sollte 250 nicht überschreiten.

Es ist eine geeignete Qualitätskontrolle zu implementieren, um mangelhafte Scanvorgänge rechtzeitig zu erkennen. Die detaillierte Ausgestaltung dieser Kontrolle soll sich am Schutzbedarf der verarbeiteten Dokumente, am Scan-Durchsatz sowie an der Zuverlässigkeit des Scansystems orientieren.

Hierzu muss die Signaturanwendungskomponente technische Vorkehrungen beinhalten, wonach der Scan-Operator gezwungen wird, einen festgelegten Stichprobenumfang einer visuellen Kontrolle zu unterziehen. Erst nach Durchführung der Sichtkontrolle der im System hinterlegten Mindeststichprobe kann der Stapel signiert werden.
Es sei besonders darauf hingewiesen, dass der Einsatz einer automatischen Signatur voraussetzt, dass die technischen Komponenten so gewählt sind, dass der Ablauf nicht unterbrochen werden kann (Transaktionssicherheit).

Es sind die allgemeinen – auch durch das BSI beschriebenen – Standards für die Herstellung der erforderlichen IT-Sicherheit für die Server und das Leitungsnetz zu beachten.

Organisatorische Vorkehrungen:
Der gesamte Verfahrensablauf vom Eingang der Papierbelege im Scan- / Signaturbereich bis zur Übertragung der Images in das elektronische Archiv sowie der Verbleib bzw. die Vernichtung der Papierbelege ist in einer Dienstanweisung (DA) detailliert zu beschreiben.

Betriebssystem und Netzwerk:
Die im Stapelsignaturgeschäft erforderlichen Sicherheitsmaßnahmen erfordern, dass das Teilnetz, in dem die für das Scannen eingesetzten IT-Systeme eingebunden und die Scan- / Signatur-Operatoren tätig sind, vom übrigen Hausnetz zu trennen ist.

Zugriff auf die Systemzeit hat ausschließlich der Administrator. Wenn dies gewährleistet wird, kann auf den Einsatz eines (kostenpflichtigen) Zeitstempeldienstes verzichtet werden.

Auf dem Rechner dürfen keine E-Mail-Programme (kein Internetanschluss) und keine Grafikbearbeitungsprogramme installiert sein.

Fernwartung:
Für eine Fernwartung sind die durch das BSI in den „IT-Grundschutz-Katalogen“ festgelegten Standards wie Call-Back-Verfahren und der Einsatz von Einmal-Passworten zu beachten. Grundlage für die zu wählenden Maßnahmen ist der jeweilige Schutzbedarf der zu scannenden Dokumente.

Darüber hinaus ist organisatorisch sicherzustellen, dass eine Fernwartung ausschließlich in Zeiten erfolgt, in denen kein Scan-Signatur-Betrieb stattfindet.

3.2.4 Vernichtung von Originalbelegen

Für die Vernichtung von Originaldokumenten / Akten gelten folgende Rechtsgrundlagen:

- § 110b SGB IV,
- § 80 SGB X,
- Art. 32 DSGVO.

Die Vernichtung der Originalpapierbelege ist in einer Dienstanweisung zu regeln. Frühester möglicher Zeitpunkt für die Vernichtung ist die vollständige elektronische Aufbewahrung und Sicherung der Images und zugehörigen Signaturen. Die Ordnungsmäßigkeit ist von der internen Revision in regelmäßigen Abständen zu prüfen.

In Fällen der „frühen Signatur“ (z. B. beim Posteingang) wird empfohlen, die papiergebundenen Dokumentationen solange aufzubewahren bis die Sachbearbeitung die Zuständigkeit geklärt hat.

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben eine datenschutzgerechte Verarbeitung der Daten sicherzustellen. Die

letzte Phase der Datenverarbeitung ist das Löschen gespeicherter Daten bzw. das Vernichten von Datenträgern. Datenträger können z. B. Festplatten, Magnetbänder, Filmmaterial, Disketten, CDs, DVDs, USB-Sticks, Chipkarten oder Papier sein.

Die datenschutzgerechte Vernichtung ist in der DIN 66399 „Büro- und Datentechnik - Vernichtung von Datenträgern“ geregelt. Verwiesen wird ebenfalls auf die Europäische Norm EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“.

Die Teile eins und zwei der DIN 66399 (gültig ab Oktober 2012) enthalten die Grundlagen und Begriffe sowie die Anforderungen an Maschinen; Teil drei DIN SPEC 66399-3 (gültig ab Februar 2013) gibt die Spezifizierung der während der Vernichtung zu beachtenden Prozessschritte vor, um so die Absicherung des Gesamtprozesses der Datenträgervernichtung zu gewährleisten.

Sozialdaten sind nach Schutzklasse 3 (sehr hoher Schutzbedarf) zu vernichten. Zusätzlich können in den jeweiligen Einsatzgebieten landes- bzw. bereichsspezifische Spezialvorschriften gelten. Die Einstufung muss sich aus wirtschaftlichen / organisatorischen Gründen immer nach dem zu vernichtenden Gut richten, welches der höchsten Schutzklasse angehört.

Zur Vernichtung von Datenträgern kann eine andere Stelle beauftragt werden. Dabei handelt es sich um einen anzeigepflichtigen Auftrag gem. § 80 SGB X. Hierbei ist zu gewährleisten, dass Sozialdaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle). Der Auftrag zur Löschung personenbezogener Daten, die Weisungen zu technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind daher schriftlich festzuhalten.

3.3 Einzelne Umsetzungsfragen

3.3.1 Umgang mit Faxsendungen

Der Prüfdienst empfiehlt die Übermittlung von Unterlagen per Fax einzustellen, da Fax-Geräte sowie Übertragungswege nicht mehr den heutigen Sicherheitsanforderungen entsprechen.

3.3.2 Verfahrensbeschreibung

Zur Beurteilung der vom SV-Träger vorgesehenen Verfahren ist die Vorlage von ausführlichen und nachvollziehbaren Verfahrensbeschreibungen unumgänglich. Solche müssen insbesondere detaillierte Informationen zu den Arbeitsabläufen (Geschäftsprozesse), den betroffenen Dokumentarten und Formularen, zu Datenschutz- und Datensicherheitsmechanismen, zur Karten- und Rechteverwaltung sowie zur Aufbewahrung, Löschung und Vernichtung beinhalten.

Der Datenschutzbeauftragte, der Informationssicherheitsbeauftragte und die Innenrevision sollten bei der Erstellung beteiligt werden.

3.3.3 Dienstanweisung

Nach § 17 SVRV i.V. mit § 40 SRVwV erlässt der Versicherungsträger bei Einsatz der automatisierten Datenverarbeitung zur Sicherheit des Verfahrens eine Dienstanweisung. Diese zur Sicherheit der Verfahren erlassene Dienstanweisung muss nach § 40 Abs. 2 SRVwV die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen sowie

die Einzelheiten zur Verwendung qualifizierter elektronischer Signaturen oder sicherer IT-gestützter Verfahren regeln. § 40 Abs. 3 SRVwV stellt weitere Anforderungen an die Dienstanweisung. Diese hat Einzelheiten zu enthalten über die Abgrenzung von Verantwortungsbereichen im Bereich der automatisierten Datenverarbeitung, Vorkehrungen für die Sicherheit bei der Datenfernübertragung und digitaler Aufzeichnung, Datenträger und Datenformat, Regelungen zu maximalen Zugriffszeiten auf Dateien, Wiederauffrischen der Daten und Berücksichtigung von technischen Veränderungen (Verfügbarkeitsanforderungen), Dokumentation zu Art und Umfang der Archivierung, und bei elektronischer Archivierung über die zusätzlich zu den Belegen zu archivierenden Angaben (insbesondere Namen des Archivierenden und Zeitpunkt der Archivierung).

Besonderheiten für den Zahlungsverkehr: Zusätzliche Regelungs- und Dokumentationsbedarfe ergeben sich nach § 40 Abs. 5 und § 41a SRVwV i. V. m. Anlage 9 zur SRVwV beim Einsatz IT-gestützter Verfahren für die Feststellung und Anordnung von Zahlungen[27] bzw. nach § 41 Abs. 1 S. 2 SRVwV beim Verzicht auf qualifizierte elektronische Signaturen.[28]

Kern dieser Anforderungen ist die Erstellung einer Gefährdungsanalyse als Grundlage der in der Dienstanweisung zu regelnden Einzelmaßnahmen.

In der Dienstanweisung sind Regelungen mindestens zu folgenden Punkten zu treffen:

Zertifikate:

- Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen (§ 15 VDG).

Kartenmanagement:[29]

- Kartenausgabe / -ersatz (bei Verlust, Zerstörung, Vergessen)
  Anmerkung: Gem. § 14 VDG kann der SV-Träger selbst – neben dem Karteninhaber – eine Sperre der Karte bzw. des Zertifikats veranlassen. Ggf. sind entsprechende vertragliche Regelungen gem. § 12 Abs. 1 VDG mit dem Vertrauensdienstanbieter zu treffen.
- Ggf. Ersatzkarten für alle Beschäftigten
- Stellvertretungsregelungen

Beschreibung des Scan- und Signaturverfahrens:

- Besonderheiten, z. B. Vorkehrungen / Regelungen zur Vermeidung von Doppelerfassungen

Zugriffs- und Zutrittsregelungen:

- Steuerung über Attributbeschreibungen / -inhalte
- Protokollierung und regelmäßige Auswertung der Zugriffe
- Zutritt zu den zentralen Scan- / Signaturarbeitsplätzen bei Einsatz der Stapelsignatur (Closed-Shop-Betrieb)

Regelmäßige Stichprobenprüfung von Signaturen:

- Täglich
- Umfang der Stichprobe, Auswahl der Stichprobe

[27] Siehe hierzu auch die Ausführungen in Abschnitten 5.2 und 6.4

[28] Die verwendeten Kategorien entsprechen denen der TR-03147 bzw. der eIDAS-Verordnung. Die eIDAS-Verordnung verwendet für die unterste Kategorie die Bezeichnung „niedrig“. Es wird an dieser Stelle jedoch die Begrifflichkeit „normal“ verwendet, die auch in der TR-03147 überwiegend verwandt wird.

[29] Siehe Ausführungen zu Punkt 3.3.4.

Verpflichtungserklärung der Beschäftigten:

- Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Der Signaturschlüssel-Inhaber muss gegenüber dem SV-Träger zustimmen, dass sein Zertifikat beim Zertifizierungsdienstanbieter abrufbar gehalten wird (§ 12 Abs. 1 VDG)
- Verhalten in besonderen Situationen, z. B. wenn die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen wird
- Prüfung arbeits- / dienstrechtlicher Konsequenzen, wenn Beschäftigte die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen haben

3.3.4 Regelungen für das Kartenmanagement

Im Rahmen des elektronischen Geschäftsverkehrs werden Signaturkarten nur an den speziellen Arbeitsplätzen benötigt, an denen die Signatur eingescannter Belege oder elektronisch erstellter Dokumente erfolgt. Diese Arbeitsplätze sind nur funktionsfähig, wenn der Bediener auf seine gültige(n) Signaturkarte(n) zurückgreifen kann.

Die Signaturkarten sollten in einem Bestandsverzeichnis verwaltet und an einem festen Platz aufbewahrt werden (z. B. in einem Schließfachsystem, aus dem die Nutzer sie bei Dienstbeginn entnehmen und bei Dienstende zurücklegen). Die Karten verlassen somit nie den gesicherten Bereich.

Besonderheiten für den Zahlungsverkehr:
Gem. § 41 Abs. 2 SRVwV sind Attributzertifikate zwingend vorgeschrieben; durch diese wird die Verwendung der Karte auf den jeweiligen Einsatzbereich beschränkt. Auf die besonderen Regelungen zur elektronischen Zahlungsanordnung § 40 Abs. 5 SRVwV wird hingewiesen.

4 Elektronische Kommunikation zwischen SV-Trägern und Versicherten

4.1 Grundsätze

Mit dem EGovG wird die elektronische Kommunikation mit der Verwaltung erleichtert. Medienbruchfreie Prozesse vom Antrag bis zur Langzeitspeicherung sind möglich.

Neben der Kommunikation über Online-Medien, gewinnt die Kommunikation über Softwareprogramme, die speziell für die Nutzung auf mobilen Endgeräten geeignet sind (Apps)[30], immer mehr an Bedeutung. Allgemein gelten die Aussagen / Grundsätze zur elektronischen Kommunikation über Online-Medien auch für die Apps.

Ab Punkt 4.2.3.7 werden daher Ausführungen zu Apps aufgenommen und Hinweise gegeben, sofern hierzu besondere Anforderungen bestehen.

4.1.1 Geltungsbereich

Gem. § 1 Abs. 1 gilt das EGovG für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Bundes einschließlich bundesunmittelbarer Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Soweit das Gesetz den Anwendungsbereich einzelner Regelungen nicht explizit auf Behörden des Bundes beschränkt, gelten sie für alle Behörden, wenn sie Bundesrecht ausführen (§ 1 Abs. 2 EGovG).

[30] Solmecke/Taeger/Feldmann (Hrsg.) Mobile Apps, Kap. 1 Rn. 14, S. 3.

Nur für Behörden des Bundes / bundesunmittelbare Körperschaften geltende Regelungen:	Für Behörden des Bundes / Landes und für bundes- / landesunmittelbare Körperschaften geltende Regelungen:
	§ 2 Abs. 1: Eröffnung eines Zugangs zur elektronischen Kommunikation
§ 2a Abs. 1: Ermächtigung zentrale Siegeldienste	
	§ 2a Abs. 2: Basisfunktion des zentrale Siegeldienstes
	§ 3: Information über Behörden und ihre Verfahren
	§ 4: Elektronische Bezahlmöglichkeiten
§ 4a: Verordnungsermächtigung für den elektronischen Rechnungsverkehr	
	§ 5: Nachweise
	§ 5a. Grenzüberschreitende Nachweisabrufe
§ 6: Ende-zu-Ende-Digitalisierung; Verordnungsermächtigung	
§ 6a Elektronische Aktenführung	
§ 7: Übertragung und Vernichtung des Papieroriginals	
§ 8: Akteneinsicht	
§ 9: Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand	
§ 9a: Verwaltungsportal des Bundes; Verordnungsermächtigung	
§ 9b: Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes	
§ 9c: Datenschutzrechtliche Verantwortlichkeit	
§ 11: Gemeinsame Verfahren	
	§ 12: Anforderungen an das Bereitstellen von Daten
	§ 13: Elektronische Formulare
	§ 14: Georeferenzierung
	§ 15: Amtl. Mitteilungs- u. Verkündungsblätter
§ 16: Barrierefreiheit	
§ 16a: Open Source	

Der Begriff der Behörde lehnt sich an die weite Definition des § 1 Abs. 2 SGB X an. Der Begriff der öffentlich-rechtlichen Verwaltungstätigkeit wird hier ebenso verwendet wie im SGB X.

Das EGovG gilt nicht, soweit Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten (§ 1 Abs. 4 EGovG). Hierunter fallen z. B. die Regelungen zur rechtssicheren Übertragung von Papierdokumenten in die elektronische Form sowie die Langzeitspeicherung elektronisch erzeugter Dokumente. Diese sind in ihrem jeweiligen Anwendungsbereich vorrangig gegenüber den in § 7 EGovG getroffenen Regelungen zum Übertragen und Vernichten des Papieroriginals.

Darüber hinaus sind insbesondere Regelungen des SGB I, SGB IV, SGB V und des SGB X sowie der DSGVO zum Sozialdatenschutz vorrangig.

Weitere Vorschriften des Sozialversicherungsrechtes, die Berührungspunkte zum EGovG enthalten, sind u.a. § 35 SGB I i. V. m. § 80 SGB X, Art. 28 DSGVO, § 36a SGB I, §§ 21, 25 SGB X.

4.1.2 Schriftformerfordernis und Ersatz der Schriftform

Nach § 126 BGB muss eine Urkunde vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden, wenn durch Gesetz die schriftliche Form vorgeschrieben ist. Der Umkehrschluss, dass immer dann, wenn eine Unterschrift vorgeschrieben ist, damit die gesetzliche Schriftform angeordnet ist, kann weder aus dem Wortlaut noch aus dem Zweck der Norm hergeleitet werden. Unterschriften werden im täglichen Leben auch außerhalb gesetzlicher Schriftformerfordernisse zu verschiedensten Zwecken geleistet und sind insbesondere als Feld für die Unterschrift des Erklärenden üblicher Bestandteil jeglicher Art von Formularen.

In den §§ 36a Abs. 2c SGB I, 13 EGovG wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird:

> *„Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.“*

Bei einer explizit angeordneten Schriftform kann in der „elektronischen Welt“ auch künftig eine Unterzeichnung **ausschließlich** über die QES oder eine der mit dem EGovG eingeführten schriftformersetzenden Technologien abgebildet werden. Die Verwendung von Pseudonymen ist nicht zulässig.

Ist eine solche Schriftform angeordnet, kann diese gemäß § 36a Abs. 2a SGB I wie folgt ersetzt werden:

Die unmittelbare Abgabe der Erklärung durch Eingabe in einem Eingabegerät der Behörde oder die Eingabe über öffentlich zugängliche Netze (z.B. Online Geschäftsstelle)

Der Identitätsnachweis muss gemäß § 36a Abs. 2a Nr. 1 Buchst. a und c SGB I über

- einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes,
- eine eID-Karte nach § 12 des eID-Karte-Gesetzes,
- einem elektronischen Nachweis nach § 78 Abs. 5 des Aufenthaltsgesetzes,
- die erfüllten Anforderungen gemäß § 9a Abs. 5 des Onlinezugangsgesetzes

erfolgen.

Zusätzlich ist gemäß § 36a Abs. 2a Nr. 1 b). SGB I für die Kommunikation zwischen dem Versicherten und seiner Krankenkasse ein Identitätsnachweis mit der elektronischen Gesundheitskarte nach § 291a SGB V oder mit der digitalen Identität nach § 291 Abs. 8 SGB V möglich.

Gemäß § 36a Abs. 2b SGB I und § 9a Abs. 2 OZG ist vor Abgabe dem Erklärenden die Gelegenheit zu geben, die gesamte Erklärung auf Vollständigkeit und Richtigkeit zu prüfen. Zudem ist der Nutzer gemäß § 9a Abs. 3 OZG durch geeignete Maßnahmen vor einer übereilten Abgabe der Erklärung gewarnt werden. Schließlich soll dem Nutzer nach § 36a Abs. 2b SGB I und § 9a Abs. 4 OZG nach Versand eine Kopie der Erklärung zur Verfügung gestellt werden.

In § 9a Abs. 5 OZG ist ein spezieller Schriftformersatz geregelt. Wenn ein Nutzer einen Identitätsnachweis über ein Nutzerkonto erbracht hat und über dieses mittels Online-Formular eine Erklärung abgibt, für die auch eine Schriftform erforderlich ist, so wird dadurch zugleich die Schriftform ersetzt.

Ferner ist Schriftformersatz möglich durch die Übermittlung einer von dem Erklärenden elektronisch signierten Erklärung an die Behörde mit der Versandart nach § 5 Abs. 5 De-Mail-Gesetzes, aus einem Anwaltspostfach nach den §§ 31a und 31b der Bundesrechtsanwaltsordnung oder aus einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach sowie aus einem elektronischen Postfach einer Behörde, einer juristischen Person des öffentlichen Rechts, einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung das nach Durchführung eines Identifizierungsverfahrens nach den Regelungen der auf Grund des § 130a Abs. 2 S. 2 der Zivilprozessordnung erlassenen Rechtsverordnung eingerichtet wurde.

Die SV-Träger müssen entsprechende Zugänge vorsehen und eine revisionssichere Speicherung eingehender Erklärungen mit Metadaten (auch Zugangsweg) sicherstellen (Integritätsschutz, siehe auch Punkt 4.3.2 und Punkt 5.2.5, zu elektronischen Verwaltungsakten siehe Punkt 4.2.2.4).

Für alle anderen Formulare, für die kein Schriftformerfordernis besteht und die der Behörde elektronisch übermittelt werden sollen, ist dies ohne Unterschrift möglich (z. B. am Bildschirm ausgefüllte PDF-Dokumente). Für diese Dokumente / Daten können jedoch erhöhte Anforderungen bzgl. des Nachweises der Authentizität des Absenders und die Integrität bei der Datenübermittlung gegeben sein (nähere Ausführungen siehe Punkt 4.2.3).

Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das Übersenden per Post sind bei Einhaltung dieser Anforderungen nicht mehr erforderlich. Sind in Papierform ausgegebene Formulare mit einem Unterschriftfeld versehen, sind diese Formulare von den Versicherten weiterhin zu unterschreiben.

4.1.3 Lesbarkeit übermittelter Dokumente

Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, übermittelt sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück (§ 36a Abs. 3 SGB I).

4.1.4 Digitale Barrierefreiheit

Nach § 16 EGovG sollen die Behörden des Bundes die elektronische Kommunikation und die elektronischen Dokumente nutzerfreundlich und barrierefrei gestalten. Nach § 7 OZG sollen Bund und Länder zudem auf eine einfache und intuitive Bedienbarkeit beim Zugang für elektronische Verwaltungsleistungen achten, sowie die Barrierefreie-Informationstechnik-Verordnung (BITV) für die barrierefreie Gestaltung heranziehen . In der BITV 2.0 werden diejenigen Vorgaben der Richtlinie (EU) 2016/2102 über die Barrierefreiheit von Websites und mobilen Anwendungen öffentlicher Stellen umgesetzt, die nicht schon 2018 in das aktualisierte Behindertengleichstellungsgesetz (BGG) aufgenommen wurden. Zudem beschreibt die BITV 2.0 den zur barrierefreien Gestaltung von Informationstechnik zu berücksichtigenden Standard nicht mehr, sondern verweist auf die im Amtsblatt der Europäischen Union bekannt gemachten harmonisierten Normen. Außerdem nennt sie Details zur Erklärung zur Barrierefreiheit und macht Vorgaben dazu, welche Inhalte barrierefrei zu gestalten sind und welche nicht. So gilt die BITV 2.0 jetzt auch für elektronische Verwaltungsabläufe (diese waren bis

zum 23. Juni 2021 barrierefrei zu gestalten). Die Anforderungen des Barrierefreiheitsstärkungsgesetzes (BFSG) sind entsprechend zu berücksichtigen.[31]

4.1.5 Datenschutzrechtliche Einschränkungen

Die mit dem EGovG eingeführten Erleichterungen bei der Übermittlung elektronischer Dokumente oder Daten erreichen dort ihre Grenze, wo es sich um besonders schützenswerte Inhalte handelt. Hierunter fallen insbesondere sensible medizinische Angaben und Dokumente (Art. 9 Abs. 1 DSGVO).

Sowohl bei der Beantwortung von Gesundheitsfragen in der Bildschirmmaske einer Web-Anwendung als auch beim Hochladen ärztlicher Dokumente können bestimmte technische Zusatzmaßnahmen der Datensicherheit und des Zugangs gefordert sein, die über die im EGovG genannten Bedingungen der datenschutzrechtlich „einfachen“ Kommunikation hinausgehen.

Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt und besondere Anforderungen an die Authentifizierung erfüllt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen.

Art. 35 DSGVO erfordert bei der Verwendung neuer Technologien die Erstellung einer Datenschutz-Folgenabschätzung. Dies gilt insbesondere dann, wenn es sich um die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) handelt (siehe Punkt 2.6).

Für den Schutzbedarf „hoch“ empfiehlt die Aufsicht des Bundesamtes für Soziale Sicherung bei Abruf von Gesundheitsdaten (z. B. Patientenquittung) aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren (z. B. Benutzername/Passwort sowie einem weiteren Sicherungsmittel wie z. B. der eID des neuen Personalausweises (nPA) / der elektronischen Gesundheitskarte - siehe Rundschreiben des Bundesversicherungsamtes vom 5. September 2014).

Der GKV-Spitzenverband hat in Abstimmung mit dem BfDI und BSI eine Richtlinie gem. § 217f Abs. 4b SGB V zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme erarbeitet.[32] Die Regelungen der endgültigen Fassung haben die Krankenkassen bei Kontakten mit ihren Versicherten anzuwenden.
Auch und in besonderer Weise gelten die Anforderungen für die Ausstellung der elektronischen Gesundheitskarte nach § 291 Abs. 6 SGB V.

Die Prüfdienste empfehlen den SV-Trägern ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung vorzusehen, z. B eine qualifizierte Zwei-Faktor-Authentifizierung

- Benutzername / Password **und**
- weiteres Sicherungsmittel wie (transaktions- oder zumindest sitzungsbezogenes) TAN-Verfahren oder – alternativ zu TAN-Verfahren - als besonders sicherem weiteren Sicherungsmittel die eGK bzw. den nPA.

---

[31] Abrufbar unter:
https://www.bundesfachstelle-barrierefreiheit.de/DE/Fachwissen/Informationstechnik/EU-Webseitenrichtlinie/BGG-und-BITV-2-0/Die-neue-BITV-2-0/die-neue-bitv-2-0_node.html
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L2102&from=DE

[32] Richtlinie zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Abs. 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) in der aktuellen Fassung abrufbar unter:
https://www.gkv-spitzenverband.de/krankenversicherung/digitalisierung/sozialdatenschutz_1/schutz_der_sozialdaten.jsp

Die Prüfdienste empfehlen, diese Vorkehrungen auch bei der Übermittlung sensibler Informationen von Versicherten an den SV-Träger vorzusehen.
Für Apps gelten die dargestellten Anforderungen in gleichem Maße. Dabei ist bei der Festlegung der Anforderungen zwischen den verschiedenen Funktionen und Inhalten von Apps zu unterscheiden:

- Anmeldung in der Online-Geschäftsstelle über die App:
  - Gleiche Schutzklassen / Anforderungen wie bei Online-Portalen
- Informationsaustausch nur über Application-Server (ohne Account bei Online-Portal):
  - Serverbasierte Schutzmaßnahmen in Bezug auf
    - Integrität der App
    - Sicherung der Übertragungswege
  - Gleiche Schutzklassen wie bei Online-Portalen
- Datenabruf vom Server (z. B. allgemeine Informationen ohne personenbezogene Daten:
  - Keine Speicherung von nicht erforderlichen Daten (Zweckbindung, Datensparsamkeit)

Zu den datenschutzrechtlichen Anforderungen an die Erstellung und das Angebot von Apps verweisen die Prüfdienste auf die Veröffentlichungen der Datenschutzbehörden.[33]

4.1.6 Zustellungsvoraussetzungen der elektronischen Gesundheitskarte

Für den Versand der eGK oder deren PIN / PUK müssen gemäß den gesetzlichen Vorgaben nach § 336 Abs. 5 SGB V und § 217f Abs. 4b S. 3 SGB V besondere Regelungen für die Zustellung getroffen werden. Bei der Ausgabe der Karte muss sichergestellt werden, dass nur der Berechtigte in den Besitz der eGK oder deren PIN / PUK gelangen darf.

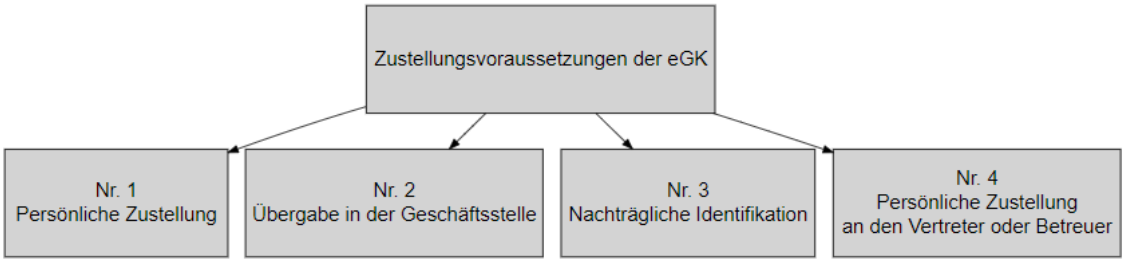

Abbildung 2 Technische und organisatorische Zustellungsvoraussetzung der eGK

[33] Z. B. Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Schwerin, 6./7. April 2016): „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ sowie Düsseldorfer Kreis der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (16. Juni 2014): „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“.

1. Persönliche Zustellung

Die Zustellung muss in einem sicheren Verfahren persönlich an den Versicherten erfolgen. Bei der Übermittlung durch die Post mit Postzustellungsurkunde ist das zuzustellende Dokument in einem verschlossenen Umschlag an die Post zu übergeben.
Für die Zustellung ist zwingend eine Auskunft aus dem Melderegister erforderlich. Die Zustellung darf nur an eine dem Versicherten zugeordnete Anschrift erfolgen. Die Melderegisterauskunft ist revisionssicher zu dokumentieren. Eine Ersatzzustellung oder eine Niederlegung ist nicht zulässig. Die Melderegisterauskunft ist entbehrlich, wenn die unter Nr. 8.2 genannten Voraussetzungen der Richtlinie des GKV-SV nach § 217f Abs. 4b SGB V erfüllt sind. Daneben sieht der Gesetzgeber weitere, nicht näher bezeichnete, sichere Verfahren zur Zustellung der eGK vor.

2. Übergabe in der Geschäftsstelle

Für die persönliche Hand-zu-Hand Übergabe ist eine Identifizierung des Versicherten anhand eines Personalausweises oder eines entsprechend sicheren Dokumentes erforderlich.

3. Nachträgliche Identifikation

Bei der Herausgabe der eGK ohne eine ausreichende Identifikation des Versicherten, ist eine nachträgliche sichere Identifikation erforderlich. Das betrifft überwiegend Versicherte, die Ihre eGK bereits vor Bekanntgabe des PDSG erhalten haben. Neben der Identifikation des Versicherten muss auch sichergestellt werden, dass sich die eGK im Besitz des Versicherten befindet. Hierzu können dem Schutzbedarf entsprechende Verfahren eingesetzt werden (siehe Punkt 4.2.3.1).

Bei Neuausgabe einer eGK ist das Identifizierungsverfahren zu wiederholen.

4. Persönliche Zustellung an den Vertreter oder Betreuer

Bei Vorliegen einer Bestellungsurkunde / Vollmacht kann auch an einen Bevollmächtigten oder einen gesetzlichen Vertreter zugestellt werden, sofern die Voraussetzungen der persönlichen Zustellung erfüllt werden.

Der Prüfdienst empfiehlt die Übergabemodalitäten der Zustellung zu dokumentieren. Daneben sind, für die persönliche Zustellung, die Melderegisterauskunft bzw. die Ausnahmegründe zu dokumentieren.

4.2 Zugang / Eröffnung der Kommunikation

4.2.1 Grundsätze

Der Austausch elektronischer Dokumente zwischen Versicherten und SV-Träger wird im § 36a SGB I geregelt. Danach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat.

Für die Kommunikation **SV-Träger → Versicherte** bedeutet dies, dass die Versicherten gegenüber dem SV-Träger ausdrücklich ihre Zustimmung für die Übermittlung elektronischer Dokumente erteilt haben müssen (§ 36a Abs. 1 SGB I). Die bloße Angabe einer E-Mail-Adresse reicht nicht aus. Gesundheitsdaten sind für den Versand per E-Mail ausdrücklich ausgeschlossen.

Dagegen ist für eine Kommunikation in Gegenrichtung **Versicherte → SV-Träger** die Bekanntgabe einer E-Mail-Adresse des SV-Trägers als Zustimmung anzusehen.

Ergänzend wird in § 2 EGovG festgelegt, wie die verschiedenen Zugänge bei den Behörden zu schaffen sind.

- Absatz 1 gibt vor, dass jede Behörde einen Zugang für die Übermittlung elektronischer Dokumente zu schaffen hat, die auch mit einer QES oder einem qualifizierten elektronischen Siegel versehen sind. Eine Festlegung auf ein bestimmtes Verfahren erfolgt hierdurch nicht. Soweit die Behörde ein E-Mail-Postfach hat, kann sie auch qualifiziert signierte elektronische Dokumente empfangen. Neben dem E-Mail-Postfach ist z. B. auch die Einrichtung eines elektronischen Zugangs über Verwaltungspostfächer oder über Online-Formulare und Web-Anwendungen möglich.

  Eine Verpflichtung zur Überprüfung einer Signatur oder zur Annahme von verschlüsselten Dokumenten wird durch das EGovG nicht begründet. Eine solche kann sich jedoch aus anderen gesetzlichen Vorschriften ergeben, z. B. aus § 110a SGB IV i. V. m. Art. 5 und 32 DSGVO.

- In Absatz 2 werden die Behörden des Bundes darüber hinaus verpflichtet, in Verwaltungsverfahren, in denen sie aufgrund einer Rechtsvorschrift die Identität der Versicherten festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachten, dies über einen elektronischen Identitätsnachweis nach § 18 Personalausweisgesetz, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten. Diese Verpflichtung ist mit Anbindung an das Bürgerkonto nach § 3 Abs. 1 OZG erfüllt.

  Bei gesetzlich Krankenversicherten kann dieser Nachweis auch mit der elektronischen Gesundheitskarte erfolgen oder mit der digitalen Identität nach § 291 Abs. 8 SGB V (§ 36a Abs. 2a Nr. 1 Buchst. b SGB I).

  Nach § 36a Abs. 5 SGB I kann die Identifizierung und Authentifizierung der Nutzer für in Ergänzung zum zentralen Bürgerkonto auch über die Nutzerkonten der Leistungserbringer erfolgen.

Hinweis:
Nur die Informationen der Versicherten, die über Verfahren gewonnen werden, die die im folgenden genannten Anforderungen an Authentifizierung, Integrität der Daten und revisionssichere Speicherung erfüllen, werden von den Prüfdiensten zu Prüfzwecken als Beleg anerkannt.

4.2.2 Zugangsmöglichkeiten bei Schriftformersatz

4.2.2.1 Qualifizierte Elektronische Signatur

§ 36a Abs. 2 SGB I regelt, dass die gesetzlich vorgeschriebene Schriftform ersetzt werden kann, sofern keine abweichende gesetzliche Regelung besteht. In diesem Fall ist das ausgehende Dokument vom Absender zwingend mit einer Qualifizierten Elektronischen Signatur (QES) nach eIDAS-Verordnung / VDG zu versehen. Die Verwendung von Pseudonymen ist hierbei nicht zulässig.

Nähere Erläuterungen zur QES enthält Punkt 3.2.2, zum Schriftformerfordernis siehe Punkt 4.1.2., zu Möglichkeiten des Verzichts auf die QES zur Ersetzung von Schriftformerfordernissen im Bereich von Rechnungswesen und Zahlungsverkehr siehe Punkt 3.3.3.[34]

[34] Siehe auch Rundschreiben des BAS vom 22. Juni 2020 „Anforderungen an IT-gestützte Verfahren des Rechnungswesens zur Ersetzung von Schriftformerfordernissen“.

4.2.2.2 Eingabe über Web-Formulare oder besondere Eingabegeräte

Eine durch Rechtsvorschrift angeordnete Schriftform kann – neben der Verwendung einer QES – auch „durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular" ersetzt werden, welches der SV-Träger „in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung stellt" (§ 36a Abs. 2a SGB I - vgl. Punkt 4.2.1).

Die Formulierung stellt klar, dass hiermit nicht elektronische Formulare gemeint sind, die die Versicherten über das Internet herunterladen, am Bildschirm ausfüllen (z. B. ausfüllbares PDF-Formular) und anschließend ausdrucken und an den SV-Träger schicken. Die Regelung betrifft die „Direktausfüllung", also die unmittelbare Eingabe von Daten in eine vom SV-Träger zur Verfügung gestellte unveränderbare elektronische Maske (Formular). Die Eingabe kann erfolgen über Web-Anwendungen oder in vom SV-Träger zur Verfügung gestellten Eingabegeräten (z. B. in seinen Kundenzentren)[35]. Die elektronische Anwendung fungiert wie ein Formular, das aus der Ferne ausgefüllt wird.

Empfehlung: Der SV-Träger sollte durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können.

Die Versicherten müssen sich vor der Nutzung authentifizieren (Authentifizierung – vgl. Punkt 4.2.3.1). Der SV-Träger hat dabei insbesondere sicherzustellen, dass die von Versicherten eingegebenen Erklärungen (Daten) mit den Identifikationsdaten des nPA / der eGK („Metadaten", z. B. Personalausweisdaten, Eingabezeit) dauerhaft verknüpft werden. Abgeleitet aus § 110a SGB IV i. V. m. Art. 5 und 32 DSGVO sind diese Daten revisionssicher zu speichern.

Die technische und organisatorische Ausgestaltung des Gesamtverfahrens (von der Eingabe durch die Versicherten bis zur Übergabe der Daten an die Fachanwendung und das Langzeitarchiv) ist in einer ausführlichen Verfahrensbeschreibung zu dokumentieren. Hierzu gehört auch die Beschreibung des Verfahrens zum Auslesen der über die Web-Anwendung eingegangenen Daten/Dokumente (einschließlich Metadaten).

In der Verfahrensbeschreibung sind insbesondere die erforderlichen technischen Sicherheitsstandards zu beschreiben. Der SV-Träger hat hierbei u. a. die datenschutzrechtlichen Vorschriften sowie die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgestellten Grundsätze zur Datensicherheit zu beachten.

Der SV-Träger hat sicherzustellen, dass neben der Eingabe über Web-Formulare den Versicherten immer auch die (herkömmliche) Papierform als alternative Möglichkeit angeboten werden muss.

Vor Abgabe ist dem Erklärenden die Gelegenheit zu geben, die gesamte Erklärung auf Vollständigkeit und Richtigkeit zu prüfen, und nach Versand ist eine Kopie der Erklärung zur Verfügung zu stellen.

4.2.2.3 Kommunikation mit De-Mail

Die De-Mail wurde als sichere und rechtsverbindliche Alternative zur „klassischen" E-Mail eingeführt; sie hat sich in der Praxis kaum durchgesetzt. Aktuell findet die De-Mail nur noch vereinzelt Anwendung, und ihre Bedeutung beschränkt sich auf wenige gesetzliche Verweise. In § 36a SGB I wird die Möglichkeit der Nutzung der De-Mail im Verwaltungsverfahren

[35] Eine Überlassung von elektronischen Eingabegeräten (z. B. Kartenleser) für Versicherte durch den SV-Träger ist gem. § 30 Abs. 1 SGB IV nicht zulässig.

erwähnt.

4.2.2.4 Versand elektronischer Verwaltungsakte durch SV-Träger

Gemäß § 9a Abs. 6 OZG kann eine durch Rechtsvorschrift angeordnete Schriftform bei elektronischen Verwaltungsakten und sonstigen elektronischen Dokumenten der Behörde, die an das Postfach eines Nutzerkontos übermittelt werden, auch dadurch ersetzt werden, dass diese mit dem qualifizierten elektronischen Siegel der Behörde versehen werden.

Nach § 36a Abs. 2a Nr. 3 SGB I kann bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde die Schriftform ersetzt werden, wenn durch ein qualifiziertes elektronisches Siegel der Behörde oder durch Versendung einer De-Mail-Nachricht nach § 5 Abs. 5 De-Mail-Gesetz, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt.

Hierbei muss der De-Mail-Diensteanbieter bei seiner in der Nachricht mitzusendenden Bestätigung (der sicheren Anmeldung) auch den erlassenden SV-Träger als Nutzer erkennen lassen. Beide Daten sind als Metadaten Bestandteil der Nachricht.

4.2.2.5 Der elektronische Widerspruch bei den SV-Trägern

Zahlreiche SV-Träger sind der Verpflichtung, Widersprüche in elektronischer Form anzunehmen, bereits nachgekommen. Sofern der SV-Träger einen Verwaltungsakt in elektronischer Form erlässt, ist es erforderlich, den Adressaten in der Rechtsbehelfsbelehrung auch auf die Möglichkeit hinzuweisen, den dagegen gerichteten Widerspruch auf demselben Wege, mit anderen Worten in elektronischer Form einzulegen.
Für Widersprüche besteht nach § 84 Abs. 1 S. 1 SGG ein „echtes“ Schriftformerfordernis.

Die Entscheidung, ob der SV-Träger einen Zugang nach § 36a Abs. 1 SGB I ermöglicht, liegt nicht mehr im Ermessen des SV-Trägers[36], er ist verpflichtet einen Zugang zu eröffnen (§ 2 Abs. 1 EGovG).
Zur Wahrung der Schriftform sind gem. § 36a Abs. 2a SGB I die in Punkt 4.2.1 beschriebenen Verfahren möglich.

4.2.3 Zugangsmöglichkeiten ohne Schriftformerfordernis

Auch bei Dokumenten, für die kein Schriftformerfordernis gesetzlich festgelegt ist, kann eine Übermittlung an den SV-Träger über die elektronischen Zugangsmöglichkeiten erfolgen. In diesen Fällen ist jedoch grundsätzlich keine Authentifizierung über die in § 36a SGB I genannten Zugangsmöglichkeiten erforderlich.
Gleichwohl kann es erforderlich sein, dass die Authentizität des Absenders und die Integrität der Originaldaten und deren revisionssichere Speicherung aus anderen Gründen (z. B. für RSA-Prüfungen) nachzuweisen sind. Sollten für diese Daten die in § 36a SGB I genannten sicheren Zugangsmöglichkeiten nicht angewandt werden, muss der Nachweis der Authentizität und Integrität der Daten auf andere Weise erbracht werden. Das gesamte beim SV-Träger zur Anwendung kommende Verfahren ist in einer Verfahrensbeschreibung detailliert zu dokumentieren.

[36] vgl. auch B. Schmidt in: Meyer-Ladewig/Leitherer/Schmidt, SGG, § 84 SGG Rn. 3; SG Hildesheim v. 03.09.2020 - S 12 AS 13/19 - juris Rn. 52

4.2.3.1 Authentifizierungsverfahren - Allgemein

Bei den folgenden Ausführungen werden die Begriffe wie in der Grafik dargestellt verwandt.[37]

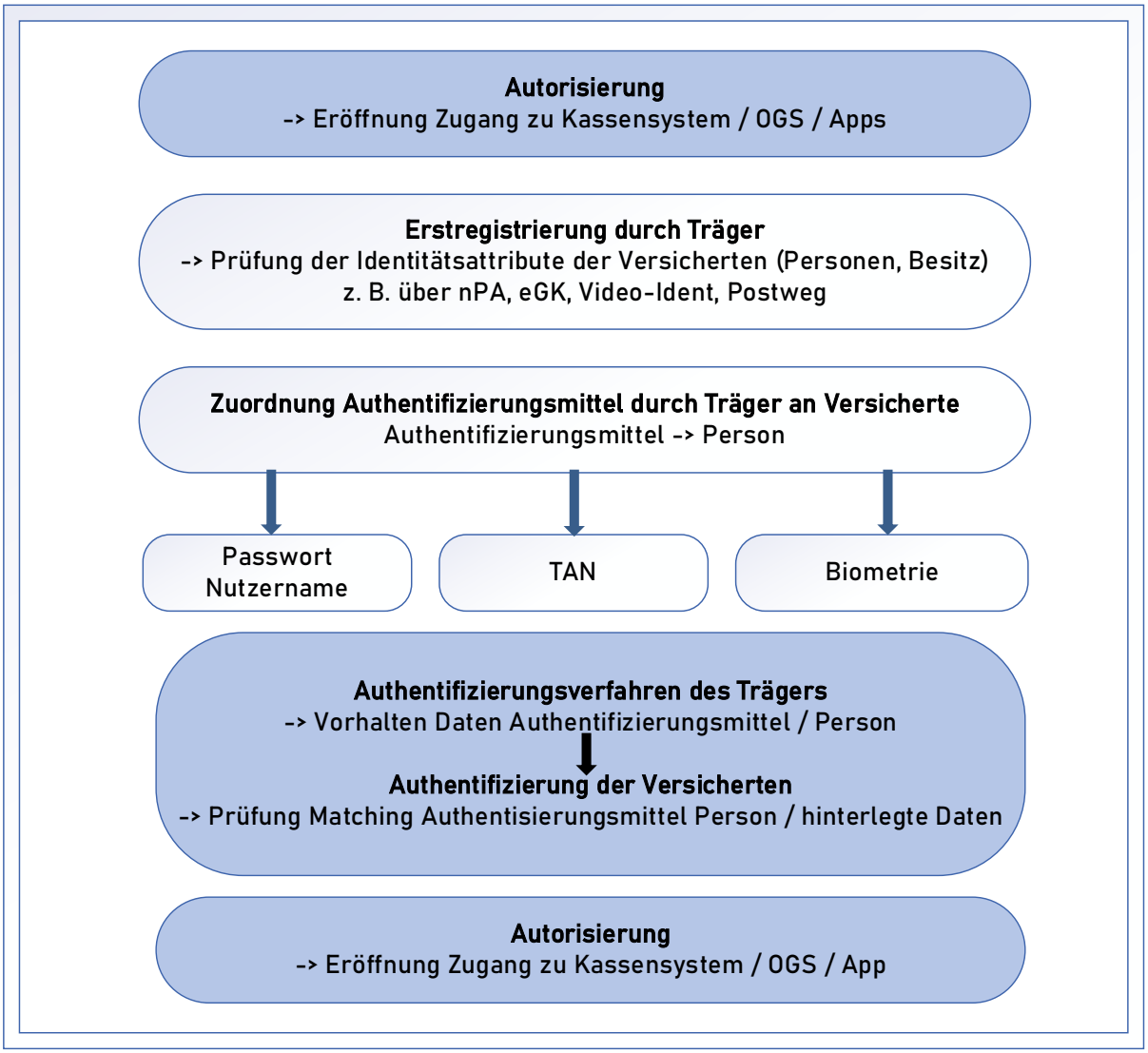

Abbildung 3 Begriffe Authentifizierungs- und Registrierungsverfahren

Zur Anerkennung von elektronisch übermittelten Daten ist die Identität des Absenders über ein Authentifizierungsverfahren festzustellen, mit dem sich die Absender mit den ihnen zugeordneten Authentisierungsmitteln im System des Trägers authentisieren und dann autorisiert auf die ihnen im System eröffneten Anwendungen entsprechend den dort vorgesehenen Rechten zugreifen können.

Schutzbedarfsfeststellung:

Bevor eine Entscheidung über die Art der Authentifizierung getroffen wird, hat der SV-Träger im Rahmen einer Schutzbedarfsanalyse festzulegen, welche Daten über das Online-Portal übermittelt bzw. abgerufen werden können.

[37] Begrifflichkeiten werden entsprechend verwandt in der Richtlinie des GKV-Spitzenverbands zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt der Krankenkassen mit ihren Versicherten nach § 217f Abs. 4b SGB V (GKV-SV Richtlinie „Kontakt mit Versicherten“)

- Je nach Schutzbedarf innerhalb des Portals sind ggf. zusätzliche Authentifizierungen für den Abruf „besonders schützenswerter“ Daten einzurichten.

- Zur Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen kann auch die TR-03147 herangezogen werden, die die Bedrohungen und Anforderungen für Verfahren zum Identitätsnachweis und zur Identitätsprüfung natürlicher Personen betrachtet.

Aus der Schutzbedarfsanalyse ergibt sich die Einstufung der elektronisch übermittelten bzw. zu übermittelnden Daten in die Sicherheitskategorien „normal“, „hoch“ und „sehr hoch“.

Hinweise zur Klassifizierung von elektronischer Eingangspost bzw. der Anzeige von Informationen innerhalb eines Online-Portals enthalten die Technische Richtlinie des BSI („TR-03138 TR- RESISCAN“) sowie das „Organisationskonzept elektronische Verwaltungsarbeit“ des Bundesministeriums des Innern. In diesen Dokumenten erfolgt die Klassifizierung des Schutzbedarfs in drei Stufen.

Je nach Schutzbedarfseinstufung der elektronischen Daten im Online-Portal oder bei der Übermittlung von Informationen ist auch das Authentifizierungsverfahren für die Nutzung einer Online-Geschäftsstelle oder App durch die Versicherten zu gestalten und einzurichten. Die nachfolgende Übersicht enthält einen groben Rahmen der Maßnahmen zum jeweiligen Vertrauensniveau:

Maßnahmen zum Schutzbedarf

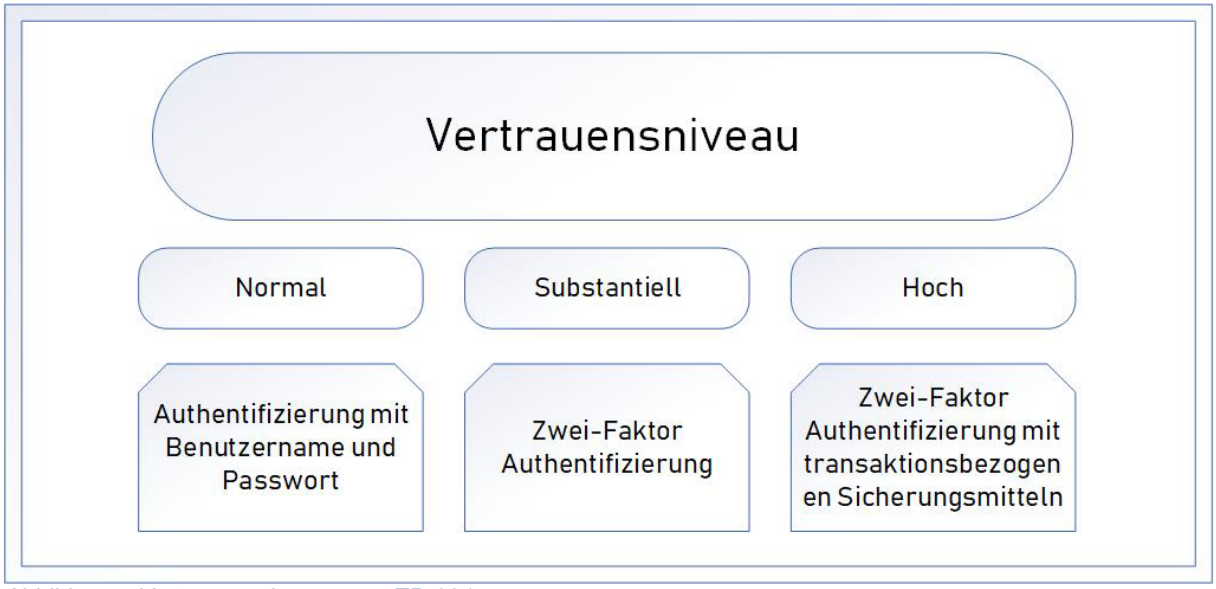

Abbildung 4 Vertrauensniveau gem. TR-03147

4.2.3.2 Anforderungen an Authentifizierung

a) Die Mindest- oder Basisanforderung für eine Authentifizierung für die Übermittlung von individuellen Informationen (persönliche individualisierte Daten), die nicht öffentlich-allgemein abrufbar sind, ist die Zwei-Faktor-Authentifizierung. Dabei enthält die Zwei-Faktor-Authentifizierung eine Kombination zweier unterschiedlicher unabhängiger Kanäle / Faktoren, die zusammen für den Identitätsnachweis eingesetzt werden.

b) Eine höhere Sicherheit kann nur erreicht werden, wenn zusätzliche Geheimnisse wie z. B. PIN und weitere Authentifizierungsfaktoren sowie kryptographische Sicherungsverfahren genutzt werden.

Dabei werden im Rahmen einer sich verändernden Authentifizierungsgrundlage[38] in der Regel kryptographische Mechanismen eingesetzt, so dass sich die zum Nachweis der Identität anzugebenden Daten bei jedem Authentifizierungsvorgang ändern.

Dabei ist von einer sicheren bzw. „starken" Authentifizierung auszugehen, wenn zusätzlich zu Elementen der Authentifizierung mindestens zwei unabhängige Faktoren eingesetzt werden.[39]

Um die Authentizität / Integrität / Vertraulichkeit der Identifikationsmerkmale während der Übermittlung zu schützen, muss vor der Übermittlung eine zwischen der Person, dem Portal und dem zusätzlichen Authentifizierungsgerät sichere Verbindung etabliert werden.
Werden Dienste über öffentliche Netze bereitgestellt, so müssen Verfahren implementiert werden, die es den Nutzern ermöglichen, die Identität des Anbieters / SV-Trägers zu verifizieren („sichere Verbindung"). Bei Web-Anwendungen kommt dazu regelmäßig eine zertifikatsbasierte Authentifizierung über TLS zum Einsatz.

Hieraus kann beispielhaft abgeleitet werden:

- Die Anzeige einer „Patientenquittung" (§ 305 SGB V) innerhalb eines Online-Portals ist - aufgrund der darin enthaltenen Gesundheitsdaten – zweifelsfrei dem Schutzbedarf „hoch" zuzuordnen.
- Für den Schutzbedarf „hoch" empfiehlt die Aufsicht des Bundesamtes für Soziale Sicherung aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren, z. B. Benutzername / Passwort sowie einem weiteren Sicherungsmittel wie z. B. der eID des nPA/der eGK.
- Eine sichere Authentifizierung über die eID des nPA bzw. der eGK wird aufgrund der bereits an sich hohen Sicherheitsstufe empfohlen. Die Möglichkeit der Nutzung der eID über eine NFC- Schnittstelle ist insbesondere bei Authentifizierung über mobile Geräte in die Überlegungen zur Ausgestaltung des Authentifizierungskonzeptes einzubeziehen. Ein sicheres Ausgabeverfahren der eGK mit eID-Funktionen bzw. der entsprechenden PIN sollte eingeplant werden, um die Funktion eines hoch sicheren Authentisierungsmittels zu ermöglichen. Die Authentifizierung mittels nPA kann z. B. anstelle eines Video-Ident-Verfahrens eingesetzt werden.[40]

Änderungen sensibler Stammdaten (Adressänderungen, Bankverbindungen etc.) sind nach Auffassung der Prüfdienste ebenfalls dem Schutzbedarf „hoch" zuzuordnen.
Die Prüfdienste empfehlen dringend, Änderungen dieser Daten durch Versicherte über elektronische Kommunikation ebenfalls erst nach einer zusätzlichen Authentifizierung vorzusehen. Hierzu kann auch ggf. das mTAN-Verfahren (wie im Bankensektor üblich, siehe auch Anforderungen des Gesetzes zur Umsetzung der Zweiten Zahlungsdiensterichtlinie „PSD2") genutzt werden.

---

[38] Im Gegensatz dazu wird unter dem Begriff „dynamische Authentifizierung" verstanden, dass die Authentifizierungstechniken abhängig von Kontext und Vorgang geändert werden (z. B. nur ein Faktor bei Login aus gesichertem Firmennetz, aber mehrere, wenn Zugriff von einem öffentlichen Hotspot aus erfolgt). Dies kann ebenfalls in einem Authentifizierungskonzept berücksichtigt werden.

[39] Siehe Art. 8 Verordnung (EU) Nr. 910 / 2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG – sog. e-IDAS-Verordnung: Sicherheitsniveau substanziell.

[40] Die technische Richtlinie TR-03128 Diensteanbieter für die eID-Funktion ist abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03128/BSI_TR-03128_Teil3.pdf?__blob=publicationFile&v=5

Die Ausgestaltung der Prozesse sollte im Kundenbereich nach der höchsten Schutzbedarfsklassifizierung „Hoch“ gerichtet werden, um später weitere Funktionen in die Anwendung leichter integrieren zu können.

c) Es wird empfohlen, ein Konzept zu Authentifizierungslösungen zu erstellen, in das die zu übermittelten / erhaltenen Informationen, deren Schutzbedarf und Authentifizierungslösungen für die einzelnen Sachverhalte aufgegriffen und Authentifizierungsmodule dargestellt werden.

Neben der Erstaufstellung sollte auch ein Verfahren zur regelmäßigen Weiterentwicklung implementiert werden.

Ein Konzept zu Authentifizierungslösungen, das die verschiedenen Schutzbedarfe berücksichtigen muss, kann modular aufgebaut sein und Module aufeinander aufbauend verbinden:

- Erstidentifikation / Erst-Authentifizierung:[41]
  Bei der Erstidentifikation können verschiedene Möglichkeiten vorgesehen werden, die wiederum unterschiedlichen „Sicherheitsklassen“ (entsprechend Schutzbedarf) entsprechen können.

- Transaktions- oder sitzungsbezogene Authentifizierungsmittel:[42]
  Auch hierbei können Authentifizierungsmittel für unterschiedliche „Sicherheitsklassen“ vorgesehen werden, die mit steigender Sicherheit auch Zwei-Faktoren-Authentifizierungsmittel darstellen.

- Nutzung eID-Funktionen:
  insbesondere der eGK / des nPA als Authentifizierungsmittel zur Erreichung des Schutzbedarfes „Hoch“.

Auch wenn die Authentifizierungsfunktionen der eGK derzeit nur über die entsprechende (Telematik-)Infrastruktur einsetzbar sind, sollten konzeptionelle Überlegungen die eGK als sehr sicheres Authentifizierungsmittel bereits berücksichtigen.

4.2.3.3 Einbeziehung von Sicherheitseinrichtungen mobiler Endgeräte

In mobilen Geräten (Smartphones) sind verschiedene biometrischen „Entsperrmethoden“ integriert, die es Nutzenden erlauben, ihre privaten Dateien vor unerlaubten Fremdzugriffen abzusichern. Die bekanntesten Methoden auf dem Markt sind derzeit der Fingerabdrucksensor und die Gesichtserkennung.

Es besteht die Möglichkeit, diese „Entsperrmethoden“ für den (dauerhaften) Zugang zu einem Online-Portal der Krankenkasse einzusetzen.

Entsprechend Punkt 4.2.3.1 bedarf es vor der Einführung eines solchen Verfahrens einer besonderen Risikoanalyse aufgrund des Schutzbedarfs der im Online-Portal übermittelten oder gespeicherten personenbezogenen Daten. Dabei sollten Versicherte darauf hingewiesen werden, dass der Zugang nur mit biometrischen Daten der jeweiligen Versicherten eröffnet werden soll.

[41] Im Sinne Verknüpfung eines „Accounts“ mit einer Person / Versicherten.

[42] Authentifizierungen, die den Zugang für die Dauer der Kommunikation („Sitzung“) bzw. für eine Handlung („Transaktion“) ermöglichen.

Weiterhin muss das biometrische Verfahren den unter Punkt 4.2.3.6.1 aufgeführten Anforderungen genügen.

4.2.3.4 Gültigkeitsdauer einer Authentifizierung

Konkrete gesetzliche Regelungen zur Gültigkeitsdauer von Authentifizierungsverfahren gibt es derzeit nicht.

Grundsätzlich sind Erstauthentifizierungen / Erstidentifikationen (Begrifflichkeiten siehe Punkt 4.2.3.1) unbefristet gültig. Sollte sich im Rahmen von Änderungen bei den Anwendungen eine Erhöhung des Vertrauensniveaus ergeben, ist ggf. eine Neu- oder Nachauthentifizierung der Versicherten erforderlich.

Die Prüfdienste empfehlen daher, stets das höchstmögliche Vertrauensniveau anzunehmen, um spätere kosten- und verwaltungsintensivere Nachauthentifizierungen zu vermeiden.

Sollte das Authentifizierungsverfahren kompromittiert worden sein, ist in Abhängigkeit vom Schutzbedarf zu prüfen, ob eine Neu- oder Nachauthentifizierung der Betroffenen oder aller Versicherten erforderlich ist.

Wurden Geräte (Besitz) als Authentifizierungsobjekt verwendet (z.B. mobile Kommunikationsgeräte wie Smartphone, Dongles etc.), sind bei Wechsel die aktuellen Geräte neu zu authentifizieren.

4.2.3.5 Eröffnung eines dauerhaften Online-Zugangs („Benutzer-Konto“)

Die Mindestanforderung der Prüfdienste für die Eröffnung eines Zugangs zum Online-Portal ist eine Zwei-Faktor-Authentifizierung.

Nach Annahme und Verifizierung der Daten durch den SV-Träger hat dieser dem Nutzer einen Freischaltcode postalisch zuzustellen. Dieser Freischaltcode ist vom Nutzer innerhalb einer vom SV-Träger festzulegenden Gültigkeitsdauer (maximal 60 Tage) bei der Erstanmeldung im Online-Portal einzugeben. Hierdurch wird das Online-Portal für Geschäftsprozesse des normalen Schutzbedarfs freigeschaltet.
Entsprechend den festgelegten datenschutzrechtlichen Sicherheitsanforderungen kann innerhalb des Online-Portals eine zusätzliche Authentifizierungsabfrage für „höherwertige“ Geschäftsprozesse notwendig werden (vgl. Punkt 4.2.3.2).

Die SV-Träger dürfen nur eine einmalige Nutzung des Freischaltcode zulassen. Lässt der Nutzer die Frist zur Ersteingabe verstreichen, muss er einen neuen Freischaltcode vom SV-Träger anfordern.

Die SV-Träger haben die technischen Voraussetzungen dafür zu schaffen, dass sowohl der von ihnen zu vergebene Freischaltcode als auch das vom Nutzer festzulegende Passwort für den Online-Zugang den Mindestanforderungen des BSI entsprechen.

Passworte, die diese Kriterien nicht erfüllen, müssen bei der Eingabe / Änderung (online) abgewiesen werden.
Der SV-Träger hat ferner festzulegen, nach wieviel Fehleingaben des Passwortes der Zugang zum Online-Portal für diesen Nutzer gesperrt wird. Üblich sind hier maximal fünf Versuche.

Bei Übermittlung von Daten der Schutzklasse „substanziell“ oder „hoch“ sollen weitere (transaktionsbezogene/sitzungsbezogene) Sicherungsmittel hinzukommen (siehe Punkt 4.2.3.2).

4.2.3.5.1 Nutzung der biometrischen Daten

Vor der Einführung eines elektronischen biometrischen Verfahrens soll eine Risikoanalyse aufgrund des Schutzbedarfs der im Online-Portal übermittelten oder gespeicherten personenbezogenen Daten vom SV-Träger durchgeführt werden.

4.2.3.5.2 Video-Ident-Verfahren

Eine (Erst-)Authentifizierung / Identifizierung für die Eröffnung des Zugangs in einem Online-Portal kann mit Hilfe eines Video-Ident-Verfahrens erfolgen.

Eine Video-Ident-Authentifizierung kann als Grundlage eines Zugangs zu einem Online-Portal mit Daten, die das Vertrauensniveau „Hoch“ aufweisen, genutzt werden. Für den Einsatz eines solchen Verfahrens ist der Anforderungskatalog für die technische Richtlinie des BSI TR-0137 in der aktuellen Fassung zu beachten.[43]

Das gesamte Verfahren des SV-Trägers soll auch unter den wirtschaftlichen Aspekten gestaltet werden. So soll das Video-Ident-Verfahren ggf. nur für die sichere Registrierung bei einem Online-Portal mit personenbezogenen Daten, die einen hohen Schutzbedarf haben, eingesetzt werden.

Auf dem Markt existieren bereits Videoidentifizierung mit automatisierten Verfahren. Diese sog. Robo-Ident-Verfahren nutzen für die Authentifizierung Module auf Basis der künstlichen Intelligenz. Ein solches Robo-Ident-Verfahren, das die speziellen Anforderungen der eIDAS, des VDG und der VDV belegt hat, wurde in die Liste der Dienste-Komponenten zur Identifizierung einer natürlichen Person bei der Bundesnetzagentur aufgenommen. Damit wird diesem Videoauthentifizierungsverfahren auf Basis der KI im Sinne von Art. 24 eIDAS die gleichwertige Sicherheit hinsichtlich der Verlässlichkeit im Vergleich zu persönlicher Anwesenheit bestätigt.

4.2.3.6 „Einmal-Kennwort-Verfahren“

Für Versicherte, die den vollen Funktionsumfang einer Online-Geschäftsstelle (noch) nicht nutzen, aber z. B. bei einzelnen Fragebogenaktionen die Antwortdaten online übermitteln möchten, bietet sich das „Einmal-Kennwort-Verfahren“ an. Die versicherte Person erhält auf dem Postweg ein Einmalpasswort, über das nur ein festgelegter Vorgang aufgerufen werden kann. Dies ermöglicht einen alternativen Zugang, ohne dass ein o.a. „Benutzer-Konto“ angelegt wird.

Das Einmal-Kennwort muss vom SV-Träger individuell für jede versicherte Person erzeugt werden. Es muss sichergestellt sein, dass das gleiche Kennwort nicht mehrfach für verschiedene Versicherte erzeugt wird. Die entsprechenden Vorgaben zur Generierung von sicheren Kennwörtern gemäß BSI sind zu beachten.

Das Einmal-Kennwort ist den Versicherten postalisch zu übermitteln. In dem Poststück ist das Eingabeverfahren zu beschreiben. Ferner ist über die festgelegte Gültigkeitsdauer des Kennwortes (max. 60 Tage) und dessen Verfall zu informieren, sobald die versicherte Person den damit verbundenen Online-Geschäftsprozess vollständig durchgeführt hat. Wird der mit dem Kennwort verknüpfte Eingabeprozess vorzeitig abgebrochen, sollte das Kennwort für eine Wiederaufnahme weiter genutzt werden können.

---

[43] Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR-03147-1_Anforderungen.pdf?__blob=publicationFile&v=5

Die vergebenen Einmal-Kennwörter sind beim SV-Träger in einer geschützten Datenbank solange zu speichern, bis der dazugehörige Prozess abgearbeitet wurde oder die Verfallfrist abgelaufen ist. Es ist sicherzustellen, dass die Sachbearbeitung zu keinem Zeitpunkt Einblick in das Einmal-Kennwort hat. Da im Zuge der Technisierung nahezu alle Mitarbeitenden eines SV-Trägers Zugriff auf die Branchensoftware mit ihrem Versichertenbestand haben, sind gegebenenfalls auch bei Rückläufern von postalisch nichtzustellbaren Einmal-Kennwort-Schriftstücken entsprechende Regelungen zu treffen.

Bei Übermittlung von Daten der Schutzklasse „Substanziell / Hoch“ können weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel erforderlich sein (siehe Punkt 4.2.3.2). Die Richtlinie des GKV-Spitzenverbandes nach § 217f Abs. 4b SGB V sieht in Anlage A unter Punkt A 5.2 vor, dass bei Verwendung eines Einmalkennwortes (lediglich) das Vertrauensniveau „Substantiell“ realisiert werden kann.

4.2.3.7 Authentifizierung bei Nutzung von Apps

Auch bei der elektronischen Kommunikation über Apps sind die allgemeinen Anforderungen zur Sicherung des Zugangs zur Kommunikation anzuwenden. Dies gilt insbesondere bei Übermittlung sensibler Daten.

Entsprechend der Schutzbedarfsfeststellung / Risikoanalyse sind die Anforderungen entsprechend dem Schutzbedarf der elektronischen Kommunikation auszugestalten. Darüber hinaus sind nachfolgende spezifische Anforderungen zu beachten:

- Eine Gerätebindung, also eine Authentifizierung des verwendeten Endgerätes kann das Sicherheitsniveau steigern.
- Gerootete Geräte sind auszuschließen.
- Für einfache Datenabrufe ohne personenbezogene Daten über einen Application-Server empfehlen die Prüfdienste, eine Nutzung der App ohne Anmeldung zu ermöglichen.
- Die App darf keine nutzerbezogenen Daten ungesichert auf dem Gerät speichern. Diese Daten sind auf dem Application-Server gesichert vorzuhalten.
- Während der Nutzung der App gespeicherte Daten sind in einem gesicherten Bereich abzuspeichern.

4.2.4 Maßnahmen bei „Identitätsverlust“

Die Prüfdienste empfehlen, trägerintern ein Verfahren für den Fall festzulegen, dass die Authentifikationsverfahren kompromittiert wurden bzw. bei Versicherten keine eindeutige Identifikation mehr möglich ist (z.B. „Identitätsdiebstahl“).

4.3 Behandlung der Online-Daten und Daten mittels Apps

4.3.1 Datenumfang und Dokumentation

Zur Übermittlung der von Versicherten eingegebenen Daten ist vor Beginn der Eingabe eine verschlüsselte Verbindung zwischen dem Eingabegerät und dem Server des SV-Trägers aufzubauen. Mindestens sind Schutzmaßnahmen zu ergreifen, die dem jeweils aktuellen Stand der Technik entsprechen, und deren kryptographische Verfahren eine angemessene Sicherheit bieten. Bei den im Rahmen der Schutzbedürftigkeit als „hoch“ oder „sehr hoch“ zu bewertenden Daten muss der SV-Träger entscheiden, ob hierbei zusätzliche Schutzmaßnahmen zu nutzen sind.

Der SV-Träger hat einen Nachweis darüber zu führen, dass die Daten durch die Versicherten übermittelt wurden (Authentifizierung, Nichtabstreitbarkeit), wann sie in seinen Zugangsbereich gelangt und dass sie dort nicht verändert worden sind (Integrität). Die empfangenen Daten lassen sich unterteilen in Nutzdaten und Metadaten:

Nutzdaten sind die von den Versicherten während des Online-Prozesses eingegebenen Angaben. Sie sind – zusammen mit der entsprechenden Frage / Bezeichnung des Eingabefeldes – zu speichern (Hinweis: Die Speicherung der „Frage“ ist als Kurzform / Schlagwort möglich).

Metadaten sind systemseitig erzeugte Zusatzdaten, anhand derer der SV-Träger belegen kann, dass die Nutzdaten durch die Versicherten erzeugt wurden. Hierzu gehören insbesondere

- eindeutiges Identifizierungsmerkmal der versicherten Person (ggf. auch Benutzername),
- Eingabeweg (Benutzer-Konto oder „Einmal-Kennwort-Verfahren“),
- Systemzeit der Übermittlung der Daten (Datum, Uhrzeit).
-

Sowohl die im Online-Prozess erhobenen Nutzdaten als auch die Metadaten sind in einer Datendatei bzw. im Fachsystem (Metadaten) revisionssicher zu speichern. Diese Daten müssen bei späteren Prüfungen (z. B. RSA-Prüfung) maschinell ausgewertet werden können. Hierzu ist es erforderlich, dass die Speicherung in einem zukunftssicheren Datenformat erfolgt. Das BSI empfiehlt hierzu u.a. das .XML- oder .csv-Format. Auch eine Speicherung als Textdatei (mit fester Satzlänge) wäre für die Prüfdienste auswertbar. Der Satzaufbau ist einheitlich zu gestalten. Fragen, die der Versicherte nicht beantworten muss, sind trotzdem aufzuführen und das Ergebnisfeld mit „blank“ zu versehen.

Neben dieser Datendatei sollte der SV-Träger aus den generierten Antworten ein PDF-Dokument erstellen, welches sich der Versicherte anzeigen und herunterladen kann. Auch dieses sollte die Nutz- und die Metadaten enthalten.

4.3.2 Integritätsschutz

Die unter Punkt 4.3.1 aufgeführten Dateien (Daten und PDF-Datei) sind unmittelbar nach ihrer Erzeugung gegen einen möglichen Integritätsverlust zu schützen. Dies kann automatisiert durch folgende Verfahren erfolgen:

- Automatische Anbringung einer QES,
- Automatische Anbringung eines elektronischen Siegels,
- Automatische Anbringung eines qualifizierten elektronischen Zeitstempels eines qualifizierten Vertrauensdiensteanbieters,
- Automatische Anbringung einer fortgeschrittenen Signatur gem. eIDAS-2.0.

Der SV-Träger hat bei der Entscheidung über die Wahl des Integritätsschutzes die Grundsätze der Wirtschaftlichkeit zu beachten. Eine Kosten- / Nutzen-Analyse (Wirtschaftlichkeitsbetrachtung) ist der Aufsichtsbehörde bei der Anzeige des Verfahrens vorzulegen. Mehr hierzu unter Punkt 2.11.

4.3.3 Revisionssichere Archivierung / Langzeitspeicherung

Die unter Punkt 4.3.1 aufgeführten Dateien (Daten und PDF-Datei) müssen unmittelbar nach Eingang beim SV-Träger / Dienstleister und vor dem Einspielen in eine Fachanwendung auf

nicht wieder beschreibbaren Datenträgern oder in einem revisionssicheren Archiv gespeichert werden.

Die Datensätze müssen während der Aufbewahrungsfristen lesbar gemacht bzw. für eine Auswertung über Prüftools zur Verfügung gestellt werden können.

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 Veränderung / Löschung von Daten sind zu dokumentieren.
Es wird empfohlen, die in der TR-03125 (TR-ESOR) des BSI enthaltenen Anforderungen an eine beweiswerterhaltende Archivierung elektronischer Daten / Dokumente zu berücksichtigen (siehe Punkt 7.3).

4.3.4 Apps

Die unter den Punkten 4.3.1 bis 4.3.3 genannten Anforderungen gelten ebenso für mittels Apps an einen Server übermittelte Daten und auf diesem Kommunikationsweg beigefügte Dokumente.
Die Software und die Datenströme sind zu beschreiben und die damit in Verbindung stehenden Anforderungen an Datenschutz, Datensicherheit, Integritätsschutz, Dokumentation und Speicherung in einer Verfahrensdokumentation festzuhalten. Die Erfüllung dieser Bedingungen ist für die Erstellung einer Datenschutz-Folgenabschätzung unumgänglich.[44]

Nur Daten für den jeweiligen Verarbeitungszweck sollten über die Apps erhoben werden, dies gilt auch für die im Rahmen sog. Tracking-Dienste zu erhebenden Daten.[45]

Eine etablierte Funktion von Apps sind die Push-Benachrichtigungen, durch die App-Anbieter mit dem Nutzenden ohne Öffnung der App in Kommunikation treten können. Sofern Push-Benachrichtigungen nicht der primäre Zweck der App sind, ist nach § 25 Abs. 1 TDDDG eine Einwilligung für den Erhalt dieser einzuholen. Der Inhalt der Mitteilung soll zweckgebunden sein und muss auf schutzbedürftige Informationen verzichten, so dass die Verarbeitung in der gesicherten Umgebung der App erfolgt.

Als Mindestanforderung an die Sicherung der Übermittlungswege ist die Absicherung der Kommunikationsverbindung App / Webserver durch eine geeignete Transportverschlüsselung vorzusehen.

Die Datenintegrität auf dem Transportweg und bei der Speicherung ist zu gewährleisten.
Nach erfolgter Schutzbedarfsanalyse sollten bei substanziellem / hohem Schutzbedarf auch kryptographische Maßnahmen vorgesehen werden.

Auf eine regelmäßige Durchführung von Updates auch durch die Nutzenden ist zu achten.

Bei der Verwendung von digitalen Gesundheitsanwendungen wird auf Punkt 8.4 verwiesen.

[44] Siehe Orientierungshilfe der Aufsichtsbehörden für Anbieter von digitalen Diensten (OH Digitale Dienste) V 1.2
[45] BAS Rundschreiben vom 21.10.2021, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-59caeb0ec6/

4.4 Elektronische Einreichung von Nachweisen

4.4.1 Einreichung durch die Versicherten

Nach § 5 Abs. 1 EGovG sind vorzulegende Nachweise (Dokumente, Bescheinigungen, Urkunden etc.) im Rahmen eines antraggebundenen Verwaltungsverfahrens elektronisch einzureichen, indem die nachweisanfordernde Stelle den jeweiligen Nachweis automatisiert bei der nachweisliefernden Stelle abruft, sofern dieser dort elektronisch vorliegt und automatisiert abgerufen werden kann, oder indem der Antragsteller den jeweiligen Nachweis elektronisch einreicht.

In § 5 Abs. 1 S. 2 EGovG wird geregelt, dass die §§ 24 bis 27 des Verwaltungsverfahrensgesetzes unberührt bleiben, also weiterhin gelten.[46] § 24 VwVfG Bund legt dabei den Untersuchungsgrundsatz fest, nach dem die Behörde Art und Umfang der Ermittlungen bestimmt. Sie kann nach § 26 Abs. 1 Nr. 3 VwVfG Bund auch Urkunden beiziehen. Daher ist die Anforderung von Unterlagen in einem Verwaltungsverfahren auch noch möglich.[47]

Die Anforderungen an die bildliche und textliche Übereinstimmung gem. § 110a Abs. 1 SGB IV sind auch an dieser Stelle entsprechend heran zu ziehen.

Für den Fall, dass Zweifel an der Echtheit der elektronischen Kopie bzw. der Übereinstimmung mit dem Original bestehen, sollte der SV-Träger die Vorlage im Original verlangen.

Die vom SV-Träger zu bestimmende Art der Einreichung umfasst auch die Frage, in welchem Format ein elektronisches Dokument einzureichen ist.

Die durch Versicherte übermittelten elektronischen Nachweise sind vom SV-Träger gegen Integritätsverlust zu schützen und revisionssicher zu archivieren.
Ein entsprechendes Risikomanagement (siehe auch Punkt 5.1.3) sollte eingerichtet werden, innerhalb dessen Dokumente nicht nur auf ihre Lesbarkeit geprüft werden, sondern stichprobenartig und in Verdachtsfällen auf ihre Echtheit. Die Träger sollten ihre Versicherten darauf hinweisen, dass Originalbelege zu diesem Zweck für einen gewissen Zeitraum aufbewahrt werden sollten. Im Rahmen des Risikomanagements sollten die Träger für sich eine Stichprobengröße festlegen, die zu Beginn / nach Einführung eines Systems größer ausfallen und im Verlauf in Abhängigkeit von den Erkenntnissen angepasst werden kann.

Es ist zu beachten, dass für Versicherte weiterhin die Möglichkeit bestehen muss, ihre Unterlagen schriftlich einzureichen.

4.4.2 Elektronische Übermittlung von Nachweisen

In § 5 Abs. 3 EGovG ist geregelt, dass die zuständige Behörde bei der Durchführung eines elektronischen Verwaltungsverfahrens erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit Einwilligung des Verfahrensbeteiligten (die Versicherten) direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen kann. Zusätzlich wird in Absatz 3 die Form der elektronischen Einwilligung festgelegt.

---

[46] Die Vorschriften des SGB sind analog anzuwenden

[47] Dies geht auch aus der Begründung zu § 5 EGovG hervor: „Nach dem verwaltungsverfahrensrechtlichen Untersuchungsgrundsatz (§ 24 VwVfG), welcher gemäß der Regelung in Absatz 1 Satz 2 ausdrücklich unberührt bleibt, kann die für die Entscheidung zuständige Behörde aber auch weiterhin die Möglichkeit haben, einen Nachweis im Original zu verlangen, sofern z. B. im Einzelfall Zweifel an der Authentizität eines Dokuments bestehen. Durch die Bezugnahme auf die §§ 24 bis 27 VwVfG wird zudem deutlich, dass die dort genannten Möglichkeiten zur Sachverhaltsermittlung bestehen bleiben. Insofern ist ein hybrides Verfahren mit elektronischen Nachweisen und analoger Beweisführung denkbar."

Nach Absatz 5 hat der Antragsteller bevor der SV-Träger den abgerufenen Nachweis verwenden darf, um die antragsgebundene Verwaltungsleistung zu erbringen, die Möglichkeit den Nachweis vorab einzusehen. Der Antragsteller kann in diesem Fall entscheiden, ob der Nachweis für das Antragsverfahren verwendet werden soll.

Für den Bereich der gesetzlichen Sozialversicherung ist der Schutz der Sozialdaten in den §§ 67 – 80 SGB X geregelt. Nach § 67a Abs. 2 SGB X sind Sozialdaten grundsätzlich beim Betroffenen (Versicherte / Mitglieder) zu erheben. Ohne seine Mitwirkung dürfen die Daten nur unter den in § 67a Abs. 2 S. 3 Nr. 1 und 2 SGB X und der DSGVO genannten Voraussetzungen erhoben werden. Die Übermittlungsbefugnis für Sozialdaten ins Ausland an Personen, Stellen oder überstaatliche und zwischenstaatliche Stellen ist in § 77 SGB X geregelt.

Da das SGB X im Verhältnis zum EGovG hinsichtlich der Erhebung von Daten gleich- oder entgegenstehende Regelungen enthält, haben diese Vorrang (§ 1 Abs. 4 EGovG). Für die Übermittlung elektronischer Nachweise zwischen SV-Trägern gelten somit die in § 5 Abs. 3 EGovG enthaltenen Bedingungen nicht. Für die Form der Einwilligung geht die in § 67b Abs. 2 SGB X enthaltene Regelung der im EGovG vor.

Das elektronische Siegel (s. Punkt 1.5) sichert die Unversehrtheit der Daten und die Richtigkeit der Herkunftsangabe. Zwar fehlt es an einer Zuordnung zu einer natürlichen Person, jedoch kann das elektronische Siegel vor allem in der Kommunikation zwischen Behörden Bedeutung erlangen.

4.5 Elektronischer Posteingang

4.5.1 Behandlung eingehender Fax-Sendungen

Der SV-Träger hat die Einsatzbedingungen über die Fax-Nutzung in einer Sicherheitsleitlinie detailliert festzulegen.

Elektronische Faxe[48]

Auch die auf einem Fax-Server eingehenden Faxe müssen – sofern keine Header- Informationen des Absenders vorhanden / sichtbar sind – mit einem elektronischen Fax-Stempel versehen werden.

Diese Faxe können wie folgt archiviert werden:

a) In Papierform (Ausdruck des Fax, s. Punkt 3.3.2 zur weiteren Speicherung) oder
b) als Image, sofern dieses nach Eingang (und ggf. Anbringung eines Fax-Stempels) und vor der ersten Zugriffsmöglichkeit durch einen Mitarbeitenden automatisch mit der qualifizierten Signatur eines (System-)Verantwortlichen oder einem qualifizierten Zeitstempel (der eine QES beinhaltet) versehen wurde (es gelten die Ausführungen zu „E-Mails“ in Punkt 4.5.2).

Hinweis:
Das unter b) beschriebenen Verfahren dient ausschließlich dem Integritätsschutz des Dokumentes.
Interne Weiterleitung von elektronischen Faxen
Die interne Weiterleitung elektronischer Faxe bzw. das elektronische Weiterfaxen an eine andere Dienststelle ist unter folgenden Voraussetzungen unkritisch:

[48] Zu Papier-Faxen siehe Punkt 3.3.1.

- Die Fax-Server befinden sich in einer gesicherten Umgebung. Zugriff hat ausschließlich der zuständige Administrator.
- Die Übermittlungswege zwischen Fax-Server und Clients sind gegen innere und äußere Eingriffsmöglichkeiten durch Unbefugte geschützt. Maßgeblich sind hier die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den BSI-Grundschutzbausteinen festgelegten Empfehlungen zur Netzsicherheit.
- Die jeweils zuständigen Beschäftigten (Fax-Server-Admin, Sachbearbeiter) verfügen über keine Bildbearbeitungssoftware, mit der der Inhalt des Fax verändert werden könnte.

4.5.2 Annahme und Speicherung eingehender E-Mails

Grundsätzlich müssen elektronisch bei dem SV-Träger eingehende Nachrichten / Dokumente, die eine rechtliche Wirkung entfalten, im elektronischen Langzeitarchiv gespeichert werden (§ 110a SGB IV). Dies gilt auch für E-Mails (Metadaten und Nutzdaten, s. 4.3.1). Voraussetzung hierfür ist, dass der SV-Träger / Dienstleister detailliert die nachfolgend genannten technischen und organisatorischen Maßnahmen festlegt und umsetzt:

- Ausführliche Verfahrensbeschreibung (einschl. Festlegung des Datenformates, z. B. automatische Umwandlung des Text in ein PDF/A-Format),
- Festlegung (im Rahmen einer Risikoanalyse), welche Dokumente per E-Mail angenommen und anerkannt werden können (insbesondere im Hinblick auf eine notwendige Authentifizierung),
- Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv,
- bei Einsatz einer Einzelsignatur (durch die Sachbearbeitung) vor der Archivierung ist ein Verfahren zu entwickeln, das eine Manipulationsmöglichkeit des Dokumentes verhindert,
- Festlegung, was mit Dokumenten zu geschehen hat, die nicht in das Langzeitarchiv gehören (z. B. unzuständiger Empfänger, SPAM, Dokumente mit extremen oder sexistischen Inhalten).

Elektronische Dokumente, die der Absender nicht qualifiziert signiert hat, sind vor der Langzeitspeicherung mit der QES eines (System-) Beschäftigten zu versehen, der für die „Betreuung“ des E-Mail- / Fax-Servers verantwortlich ist. Die Signatur kann im Wege der Massensignatur erfolgen. Alternativ ist auch eine Einzelsignatur durch den Empfänger (Sachbearbeiter) möglich. Der Integritätsschutz kann auch über die in Punkt 4.3.2 aufgeführten alternativen Sicherungsmittel erreicht werden.

Hinweis:
Die an diesen Dokumenten angebrachte Signatur dient ausschließlich dem Integritätsschutz des Dokumentes.

4.5.2.1 Über Portale / Anwendungen eingehende Nachrichten

Bei Mitteilungen / Nachrichten die über Portale oder Anwendungen eingehen sind technische Verfahren zur Authentifizierung und Übertragung der Daten vorzusehen. Der Absender muss sich jeweils am Portal bzw. der Anwendung authentifizieren („anmelden“), um eine Nachricht an den SV-Träger senden zu können. Diese Form des Übermittlungsweges bietet folgende Vorteile:

- Eindeutige Authentifizierung des Absenders,
- Anerkennung übermittelter Informationen als Beleg (z. B. bei RSA-Prüfungen),

- Eingang der Daten über einen gesicherten Übermittlungsweg (Verschlüsselung),
- Differenzierte Vorgangssteuerung über Funktionspostfächer für die Sachbearbeitung,
- Eingrenzungsmöglichkeit der Dokumentenformate und Dokumentengröße,
- Minimierung des Risikos, SPAM und andere nicht erwünschte Daten annehmen zu müssen.

4.5.2.2 E-Mail-Eingang ohne Authentifizierung des Absenders

Bei einer „normalen“ E-Mail (ohne QES) ist die Authentizität des Absenders nicht nachprüfbar. Somit kann aus dieser zunächst keine rechtliche Wirkung gezogen werden. Aufgrund der grundsätzlich bestehenden Formfreiheit kann sie jedoch für die Ingangsetzung eines Verwaltungsverfahrens herangezogen werden, in dessen Verlauf dann Angaben beweissicher erhoben werden müssen.

Enthält eine solche Mail einen Anhang, der die QES des Absenders beinhaltet, sind E-Mail und Anhang zu speichern.

4.6 Elektronischer Postausgang

4.6.1 Grundsätze

Für den Bereich der gesetzlichen Sozialversicherung gilt grundsätzlich das Prinzip der Formfreiheit. So kann der Erlass eines Verwaltungsaktes z. B. auch mündlich erfolgen (siehe § 33 Abs. 2 1 SGB X). Es müssen lediglich die in § 33 Abs. 3 S. 1 und ggf. Abs. 5 SGB X genannten Anforderungen (Erkennbarkeit der erlassenden Behörde) gewahrt werden. Dementsprechend kann z. B. bei einer Postausgangssignatur auf die QES grundsätzlich verzichtet werden.

Etwas anderes gilt nur dann, wenn für den Verwaltungsakt die Schriftform angeordnet ist. In diesem Fall sind die in § 33 Abs. 3 bis 5 SGB X genannten Voraussetzungen zu erfüllen.

Nach § 9 Abs. 1 S. 1 OZG ist für die elektronische Bekanntgabe von Verwaltungsakten über ein Postfach des Nutzerkontos weiterhin die Einwilligung des Nutzers erforderlich. Zur Vereinfachung der elektronischen Bekanntgabe und Ermöglichung der Volldigitalisierung regelt § 9 Abs. 1 S. 2 OZG eine Einwilligungsfiktion. Dies bedeutet, dass eine Einwilligung als erteilt gilt, wenn der Nutzer diese Form der Bekanntgabe bei der Inanspruchnahme von Verwaltungsleistungen nicht ausschließt („Opt-out“). Nach § 9 Abs. 1 S. 4 gilt die Bekanntgabe am vierten Tag nach der Bereitstellung zum Abruf als erfolgt.

4.6.2 E-Mails (ohne / mit Anhang)

Ausgehende E-Mails (einschl. Anhänge) sollten in einem revisionssicheren Speichersystem / Langzeitarchiv unveränderbar gespeichert werden. Zur Sicherung der Integrität der Dokumente sollte ein entsprechender elektronischer Integritätsschutz (Punkt 4.3.2) angebracht werden.

Bei ausgehenden E-Mails[49] hat der SV-Träger unbedingt darauf zu achten, dass diese E-Mail keine personenbezogenen Daten / Sozialdaten enthält. Verwiesen wird auf die Orientierungshilfe der DSK zu den Maßnahmen zum Schutz personenbezogener Daten bei der

[49] Unverschlüsselt oder nicht authentifiziert

Übermittlung per E-Mail vom 16. Juni 2021.[50]

Eine Einwilligung der Versicherten in den Versand unverschlüsselter E-Mails mit personenbezogenen Daten ist nicht zulässig.

4.6.3 Erstellung und Versand von Serienbriefen

Im Rahmen von elektronischen Workflows ist es üblich, Serienbriefe unter Verwendung vorgefertigter Textbausteine, z. B. als Bescheide, zu versenden. Aufgrund der Regelungen in § 110a SGB IV ist zu empfehlen, bei der Langzeitspeicherung die „Durchschriften“ derartig erzeugter Briefe mit einer QES des Absenders (oder einem alternativen Integritätsschutz gem. Punkt 4.3.2) zu versehen. Nach § 110a Abs. 2 S. 3 SGB IV ist es bei der Langzeitspeicherung nicht erforderlich, dass die Wiedergabe auf dem dauerhaften Datenträger mit der erstellten Unterlage (Brief an Versicherte) bildlich übereinstimmt. Das bedeutet, dass die elektronische „Durchschrift“ z. B. unter Aufführung der verwendeten Textbausteinnummern sowie der Variablen erfolgen kann. Die inhaltliche Übereinstimmung mit dem ursprünglich versandten Brief muss jedoch nachvollziehbar sein.

Im Rahmen der zunehmenden Verwendung von E-Akten ist es auch möglich, die Einzeldokumente in der jeweiligen E-Akte abzulegen.

Auf die Ausführungen im Abschnitt 5 „Automatisierte Sachbearbeitung“ wird verwiesen.

4.7 Soziale Netzwerke

Bei der Verwendung von Messaging- bzw. Kurznachrichtendiensten sowie sozialen Netzwerken zur Kommunikation mit Versicherten sind die vom Bundesversicherungsamt mit Schreiben vom 18.08.2017 bekannt gegebenen Grundsätze zur Einhaltung des Datenschutzes und der Datensicherheit zu beachten.[51] Weitere Ausführungen enthält auch die Bestandsaufnahme des Digitalausschusses des Bundesamtes für Soziale Sicherung unter Beteiligung des Prüfdienstes.[52]

Zur Präsenz von Trägern auf entsprechenden Plattformen s. Punkt 8.3.

[50] Abrufbar unter: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

[51] Abrufbar unter https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/2017-08-18_Rundschreiben_Soz-Netze_MessagingDienste.pdf

[52] Abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/ki-big-data-cloud-computing-und-automatisierte-bearbeitung/webkonferenz-und-messaging-dienste.

5 Automatisierte Sachbearbeitung

5.1 Einleitung

Die (teil-)automatisierte Sachbearbeitung ist eine Form der automatisierten Datenverarbeitung, bei der die Verarbeitung von Sachverhalten (teilweise) ohne Unterstützung oder gleichzeitigen Zugriff durch eine natürliche Person sich selbst organisierend und anhand vorgegebener technischer wie fachlicher Parameter abläuft. Von einer sog. „Dunkelverarbeitung“ wird gesprochen, wenn der Prozess vom Eingang der Daten bis zur Entscheidung (Feststellungsverfahren, Zahlungsanweisung etc.) und ggf. Versendung der Entscheidung an andere Stellen gänzlich ohne Zugriff natürlicher Personen abläuft.

Da durch die Automatisierung von Arbeitsabläufen Prozesse effizienter, schneller und kostengünstiger durchgeführt werden können und sollen, wird teil- oder vollautomatisierte Sachbearbeitung bereits bei vielen SV-Trägern in unterschiedlichem Umfang und unterschiedlichen Geschäftsfeldern angewendet. Die automatisierte Datenverarbeitung unterliegt im Hinblick auf die Ordnungsmäßigkeit der durch die Verarbeitung abgewickelten Geschäftsvorfälle und Prozesse besonderen Anforderungen.

Rechtsvorgaben / Hilfen / Unterlagen

- § 31a und § 37 SGB X
- § 110a SGB IV mit Grundsätzen der Aufbewahrung des GKV-Spitzenverbandes
- SVRV / SRVwV

5.2 Anforderungen

Ziel der Umsetzung der untenstehenden Anforderungen ist, dass die Verfahren fachlich und technisch rechtmäßig sowie wirtschaftlich ablaufen und die grundlegenden Informationen (Originaldaten und Ergebnisse) als Belege Anerkennung finden können. Hierzu dienen die im Folgenden angeführten Anforderungen, die bei Einrichtung und Betrieb von Anwendungen der automatisierten Sachbearbeitung einzubeziehen sind.

5.2.1 Materielles Fachrecht

Das auf die Sachverhalte anzuwendende Recht ist in vollem Umfang auch bei automatisierten Schritten der Bearbeitung zu beachten.

- **SVRV / SRVwV**
  Die Vorschriften der Rechnungslegung (insbesondere die Regelungen der SVRV und der SRVwV) sind auch bei automatisierter Sachbearbeitung zu beachten.
  Zu nennen sind insbesondere die Vorgaben zu Zahlungsanordnung und Zahlungsfreigabe, Bestätigung der Vollständigkeit sowie rechnerischen und sachlichen Richtigkeit der Prozesse, die in entsprechender Weise technisch umzusetzen bzw. abzubilden sind (siehe weitere Ausführungen dazu unter Punkt 5.3 und 6.4).

  Das Verfahren ist in der Kassenordnung (siehe § 3 SVRV, § 8 SRVwV) sowie in einer Dienstanweisung (siehe § 17 SVRV) zu beschreiben.

- **Anforderungen an Verwaltungsakte**
  Die Anforderungen an Verwaltungsakte im Rahmen der automatisierten Sachbearbeitung ergeben sich nach jeweiligem Erstellungsprozess, Form und Bekanntgabe von Verwaltungsakten:

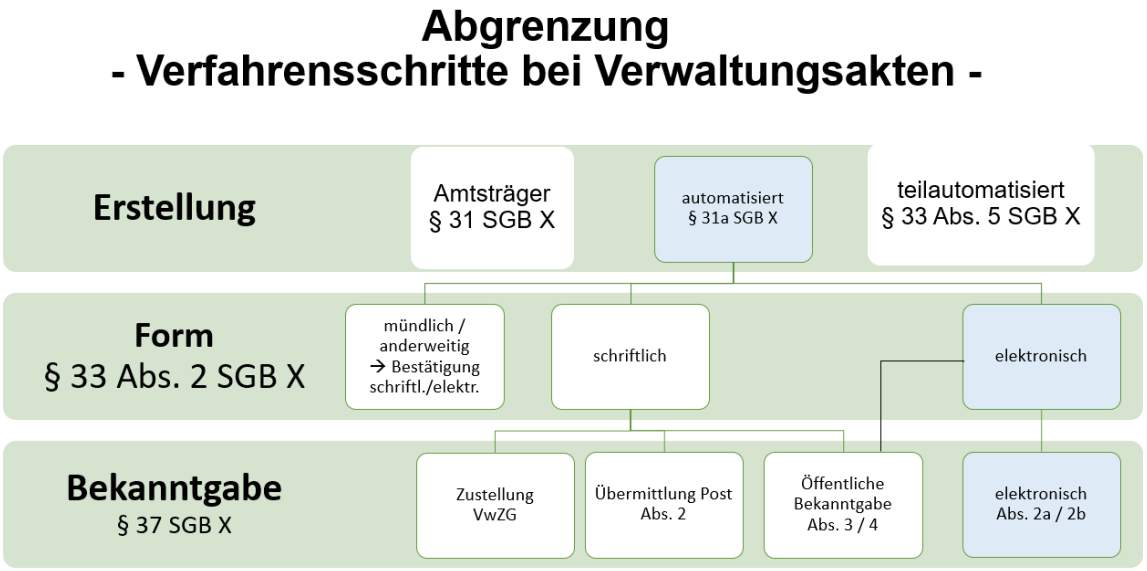

Abbildung 5 Übersicht Formen Verwaltungsakt

- **§ 31a SGB X**
  Der vollständig automatisierte Erlass von Verwaltungsakten als eine Erscheinungsform / ein Anwendungsfall der vollautomatisierten Sachbearbeitung ist (nur) unter bestimmten Bedingungen möglich:

  - So darf im Verfahren der Entscheidung zum Verwaltungsakt keine Bearbeitung durch einen Amtsträger erforderlich werden.
  - Die Vorschriften des SGB X sind einzuhalten.

  Dies bedeutet, dass für die Anwendung des § 31a SGB X eine Datengrundlage vorhanden sein muss, die bereits an sich einen entscheidungsrelevanten und -reifen Sachverhalt abbildet und keine komplexe Entscheidungslagen vorliegen, die eine Bearbeitung durch Amtsträger erforderlich macht. Eine komplexe Lage kann insbesondere bei Entscheidungsalternativen, Bewertungen, Ermessensspielräume, Plausibilitätsprüfung von Angaben etc. vorliegen. Eine eindeutige, strikte Schematisierung der Entscheidungsfindung, die keine weitere Entscheidung einer natürlichen Person als Sachbearbeitung mehr benötigt, muss daher gegeben sein.

  Auch die Berücksichtigung tatsächlicher Angaben Betroffener muss im Verfahren möglich sein. Diese sind, wenn sie bedeutsam sind, auch im Verwaltungsakt zu würdigen. Es sollten daher Freitextfelder bei der elektronischen Eingabe von Informationen durch Betroffene vorgesehen werden (bei Anträgen etc.). Diese Angaben sind dann auf ihre Bedeutung für die Entscheidung des Trägers zu würdigen (wenn nicht maschinell möglich, dann durch Amtsträger).

- **§ 33 SGB X**
  Neben der (voll-)automatisierten Erstellung von Verwaltungsakten nach § 31a SGB X ist auch eine teilautomatisierte Erstellung nach § 33 Abs. 5 SGB X möglich. Hierbei greifen

Besonderheiten bei Unterschrift und Namenswiedergabe. Bei in der Form elektronischen Verwaltungsakten muss das der Signatur zu Grunde liegende Zertifikat nur die erlassende Behörde erkennen lassen, eine (persönliche) Signatur des Amtsträgers ist nicht erforderlich.

- **§ 37 Abs. 2a SGB X**
  Eine elektronische Bekanntgabe von Verwaltungsakten ist nach § 37 Abs. 2 S. 2 Abs. 2a bzw. 2b SGB X[53] i. V. m. § 9 OZG möglich. Vorteil der elektronischen Bekanntgabe sind die jeweiligen Zugangsfiktionen der Alternativen. Bei der Umsetzung der technischen Möglichkeiten sind jedoch Anforderungen zu beachten, damit die Risiken der Beweislast bei Bestreiten des Zugangs reduziert werden.

  Als allgemeine Voraussetzung aller Alternativen der elektronischen Bekanntgabe muss die Übermittlung elektronischer Dokumente nach § 36a Abs. 1 SGB I zulässig sein. Dies schließt ein, dass die Empfänger hierfür einen Zugang eröffnet haben und dies auch für den Bereich der Bekanntgabe von Verwaltungsakten zulässt (Widmung):

  - De-Mail-Postfach bei Fremdanbieter,
  - Nutzung einer Online-Geschäftsstelle / App des Trägers (hierbei sollte eine Einwilligung zur Nutzung dieses Weges auch für die Bekanntgabe von Verwaltungsakten eingeholt werden),
  - Online-Postfächer Drittanbieter.[54].

  Die Form der Bekanntgabe wird durch § 37 Abs. 2 SGB X nicht vorgegeben, so dass die Behörde nach ihrem Ermessen über die schriftliche oder elektronische Form bestimmen kann.[55] Unter einer Absendung als elektronische Form ist der sichere leitungs- oder webbasierte Datentransfer zwischen zwei elektronischen Rechnern zu verstehen. Eine in diesem Sinne sichere Übermittlung an authentifizierte Personen erfolgt über De-Mail im Sinne des § 36a Abs. 2a Nr. 3 d) SGB I.

  Das Verfahren nach § 37 Abs. 2a SGB X sieht die Bereitstellung des elektronischen Verwaltungsaktes zum Abruf über öffentliche Netze vor, z.B. über Portale, Online-Geschäftsstellen oder Apps. Dabei sind folgende Schritte in die Gestaltung der entsprechenden Trägerverfahren einzubeziehen:

  - eine (jederzeit mit Wirkung für die Zukunft widerrufbare) vorherige Einwilligung der Versicherten in elektronische Kommunikation und insbesondere in die elektronische Bekanntgabe von Verwaltungakten; die Einwilligung ist vom Träger nachweisbar vorzuhalten,
  - Einstellung des Verwaltungsaktes in Portal / Online-Geschäftsstelle / App,
  - elektronische Benachrichtigung an vorab identifizierte elektronische Adresse des Adressaten über die Bereitstellung im Portal [56],
  - sichere Authentisierung der Adressaten bei Zugriff auf das Portal / Online-Geschäftsstelle / App,
    Für den Zugriff auf das Portal / Online-Geschäftsstelle / App sind insbesondere

[53] In der Fassung des Gesetzes zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen vom 03.12.2020; BGBl I Nr. 59 vom 09.12.2020, S. 2668.
[54] Datenschutzrechtlich bleibt der Träger verantwortlich, eine „Auslagerung“ der Verantwortung für Verarbeitungsschritte in die Sphäre der Versicherten erfolgt nicht.
[55] Siehe Digitalausschuss im BAS abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/digitaler-kundenservice-und-automatisierte-bearbeitung/bekanntgabe-eines-verwaltungsakts/

bei deren Nutzung auch für die Bekanntgabe von Verwaltungsakten geeignete Identifizierungsmittel zu nutzen, um die Authentisierungsmittel für den Einzelzugriff zuzuordnen. Dabei ist davon auszugehen, dass die Inhalte von Verwaltungsakten regelmäßig den Vertrauensniveaus substanziell und hoch zuzuordnen sind. Die Handreichung des IT-Planungsrates sieht für die Dokumentenübermittlung über Web-Upload für das dort verwandte Vertrauensniveau hoch+ z. B. die Nutzung der eID-Funktion des Personalausweises vor. Entsprechend sind auch die Authentifizierungsmittel – ggf. innerhalb eines Modulsystems - zu wählen (siehe Punkt 4.2 „Authentifizierung“),

- Speicherbarkeit des elektronischen Verwaltungsaktes für Adressaten in deren EDV-Systemen in gängigen Dateiformaten,
- Protokollierbarkeit des erstmaligen Abrufs des Verwaltungsaktes vom Portal,
- Empfohlen: Aufbau eines Verfahrens, um nach Abs. 2a S. 8 das Bekanntgabeverfahren ggf. wiederholen bzw. wechseln zu können (z.B. bei technischen Problemen des Abrufs, Bestreiten der Einwilligung oder des Zugangs der Bereitstellungsnachricht).

Alternativ zur elektronischen Benachrichtigung über DE-Mail kann auch folgender Schritt vorgenommen werden (die weiteren oben genannten Schritte müssen natürlich eingehalten werden):

- ausdrückliches vorheriges Einverständnis der Adressaten zu einer Bereitstellungsbenachrichtigung zum Abruf:
  - durch z.B. eine unverschlüsselte, aber in diesem Zusammenhang vorab identifizierte E-Mail-Adresse oder
  - über eine App, zu der ein authentisierter Zugang der Adressaten gegeben ist.

Für beide Alternativen gilt, dass neben der Authentifizierung bei Übermittlung die entsprechenden Konzepte auch eine sichere Benachrichtigung über die Bereitstellung des Verwaltungsaktes vorsehen sollte. Dabei sollten bereits hierbei sichere Identifikationslösungen bei Vergabe der Authentisierungsmittel vorgesehen werden:

- Nachweismöglichkeit des Trägers zum Zugang der Benachrichtigung (Bekanntgabe dann zu diesem Zeitpunkt) bzw. – wenn dies nicht möglich bzw. ergänzend – Nachweis des tatsächlichen Abrufs des Verwaltungsaktes. Die Speicherung der durch die Versicherten erfolgten Abrufe hat seitens der SV-Träger zu erfolgen und die entsprechenden Abrufdaten sind revisionssicher zu speichern (Nachweis des Zugangs).

5.2.2 Dokumentation zur automatisierten Sachbearbeitung

Die automatisierte Sachbearbeitung stellt besondere Anforderungen an die Dokumentation, insbesondere da einzelne Arbeitsschritte in konkreten Verfahren nur über die parametrisierten Programmierungen erklärbar sind.

- Die grundlegenden Einstellungen (Parameter) der automatisierten Sachbearbeitung und die einzelnen Schritte der Sachbearbeitung (automatisiert sowie manuell) im konkreten Sachverhalt / Fall müssen nachvollziehbar für einen Dritten außerhalb des Systems des SV-Trägers (sachverständige Dritte) erkennbar sein.

- Verarbeitungsvorgänge sind (automatisch) zu protokollieren. Diese Protokollierung umfasst die Verarbeitungsschritte und Verarbeitungsdaten selbst sowie die dazugehörigen sog. Metadaten (insbesondere: Wer hat wann welchen Prozess angestoßen bzw. welcher automatisierte Verarbeitungsschritt hat wann mit welchem Versionsstand gegriffen).

- Fehler und Verarbeitungsabbrüche sind zu dokumentieren. Der zuständige Fachbereich des SV-Trägers sollte die Fehler und Verarbeitungsabbrüche im Hinblick auf ggf. bestehenden Anpassungsbedarf auswerten.
  Die Dokumentation kann insbesondere im Rahmen des internen Qualitätsmanagements bzw. der Prüfungen des Internen Kontrollsystems (IKS) herangezogen werden.
- Seit dem 01.01.2019 ist es nach den Vorschriften der SVRV und der SRVwV möglich, bei IT-gestützter, automatisierter Feststellung und Anordnung von Zahlungen und Buchung auf den kostenintensiven Einsatz qualifizierter elektronischer Signaturen zur Ersetzung der Schriftform zu verzichten. Voraussetzung hierfür ist der Einsatz dokumentierter, hinreichend getesteter und freigegebener Programme. Zu diesem Zweck ist eine Verfahrensdokumentation einschließlich einer Gefährdungsanalyse und eines Ordnungsmäßigkeitskonzeptes zu erstellen; die Details sind in einer Dienstanweisung zu regeln. [57]
  Es muss eine (revisionssichere) Archivierung der Verarbeitungsdokumentation erfolgen (Verarbeitungsdaten und Metadaten hierzu).

5.2.3 Kontroll- und Prüfungsumfeld / Risikomanagement

Die automatisierte Sachbearbeitung (Aufbau und Betrieb) erfordert einerseits deren Einbeziehung in das „normale“ Umfeld der Kassenverfahren (siehe auch Abschnitt 1), andererseits aber auch spezielle, aus der Besonderheit der technischen Datenverfahren resultierende Anforderungen in fachlicher und organisatorischer Hinsicht.

- Fachliche Anforderungen
  Die fachlichen Anforderungen, die an das interne Prüf- und Kontrollumfeld einer „normalen“ Sachbearbeitung zu stellen sind, sind auch bei einer automatisierten Sachbearbeitung zu erfüllen. Dies gilt für das materielle Fachrecht ebenso wie für die Vorschriften der Rechnungslegung (siehe oben).

- Umsetzung der Anforderungen des Internen Kontrollsystems
  Die automatisierte Sachbearbeitung ist auf die Vorgaben des IKS einzustellen.
  Das Interne Kontrollmanagement seinerseits hat die Verfahren der automatisierten Sachbearbeitung in ihren allgemeinen wie speziellen Anforderungen in das Kontrollkonzept und Prüfgeschehen einzubeziehen.

- Risikomanagement
  Verfahren der Digitalisierung und Automation sind mit besonderen (Daten-)Risiken verbunden. Daher sind diese Verfahren vor Errichtung und bei Betrieb im Rahmen eines Risikomanagements besonders zu betrachten (siehe Abschnitt 1 „Risikomanagement“).
  Bei Verfahren der automatisierten Sachbearbeitung sind im Rahmen des Risikomanagements insbesondere Fragen zu Risiken bei der Verarbeitung von Daten (Datenverlust, Erreichbarkeit der Daten, Übermittlung von Daten an Stellen außerhalb des Systems des SV- Trägers) sowie die organisatorische Lauffähigkeit des Systems bzw. der konkreten Anwendung (Ausfallsicherheit, Arbeitsfähigkeit etc.) zu betrachten.

- Notfallmanagement
  Das Notfallmanagement (Business Continuity Management) ist aufzubauen bzw. bestehende Verfahren sind ggf. im Hinblick auf die neuen Verfahren der automatisierten Sachbearbeitung anzupassen.

[57] Auf die vom BAS erlassenen Hinweise zur Erstellung einer Arbeitshilfe zur „Anforderung an IT-gestützte Verfahren des Rechnungswesens zur Ersetzung des Schrifterfordernisses“ vom 22.06.2020, die dem Rundschreiben des GKV-SV, RS-2020/478 vom 24.06.2020 beiliegt, sowie speziell zur Zahlungsfreigabe auf Punkt 5.3.1 wird hingewiesen.

- Verantwortlichkeit
  Für die einzelnen fachlichen Geschäftsprozesse, die mit Verfahren der automatisierten Sachbearbeitung unterstützt werden sollen, sind die fachlichen und technischen Verantwortlichen und deren Aufgaben bereits im Vorhinein festzulegen.
  Dies gilt auch für die Ausgestaltung der Verfahren der automatisierten Sachbearbeitung selbst. So ist die Verantwortung für die Festlegung der einzelnen fachlichen Parameter nachvollziehbar zu dokumentieren.

- Festlegung der Zugangs- und Zugriffsberechtigungen
  Gerade bei einer automatisierten Sachbearbeitung sind die Zugangs- und Zugriffsberechtigungen sowie die Möglichkeiten zur Änderung fachlicher Parameter sorgfältig festzulegen und einzurichten (Rechte- / Rollen- / Nutzerinnenkonzept). Bei diesen Verfahren besteht aufgrund der möglichen Vielzahl der mit den Anwendungen automatisiert bearbeiteten Sachverhalte ein erhöhtes Risikopotential.

  Das Konzept und seine Ausführung (Rechtevergaben, Nutzung der Rechte) sind im Verlauf – als Teil des IKS - zu kontrollieren. Diese Kontrollansätze sollten bereits bei Einrichtung der Anwendung / des Systems aufgebaut werden.

- „Manuelle“ Stichprobenprüfung
  Eine automatisierte Sachbearbeitung kann sich auf eine Vielzahl von Fällen / Sachverhalten auswirken. Dabei müssen im Vorhinein der fachliche Prozess und die auf ihn bezogenen fachlichen und technischen Parameter festgelegt werden. Daher können fehlerhafte bzw. nicht sinnvolle Parametersetzungen große Auswirkungen haben.

  Insbesondere mit Blickrichtung auf die Erfüllung der fachlichen Anforderungen sind daher neben der Prüfung fachlich auffälliger Fälle, die die Anwendung bereits identifiziert, regelmäßige Stichprobenprüfungen auf die Einhaltung der fachrechtlichen Vorgaben vorzusehen. Die Höhe der Stichproben sollte risikoorientiert festgelegt werden. Parameter hierfür können sein
  - die Zahl der verarbeiteten Einzelprozesse und die Komplexität des Verfahrens (je komplexer das Verfahren desto höher die Fehleranfälligkeit); eine Stichprobe sollte Erkenntnisse aus den verschiedenen Schritten des Verfahrens ermöglichen, z.B. im Rahmen einer geschichteten Stichprobe
  - die Auswirkung des automatisierten Verfahrensschrittes / Verfahrens (Zahlung, Höhe der Zahlung, finanzielle Auswirkungen, Bedeutung für die Versicherten wie Leistungsgewährung etc.)
  - weitere Prozesse der Träger, die an den Informationen aus dem Verfahren hängen (bei ggf. sogar automatisierter Weiterarbeit mit den Ergebnissen in anderen Prozessen ergibt sich Risiko auch für diese nachgelagerten Prozesse)
  - Auswirkungen im Schadensfall (finanziell, Öffentlichkeitswirksamkeit).

  Bei fachlich auffälligen Fällen sollten, sofern sich die Auffälligkeit aus von den Versicherten zur Verfügung gestellten Informationen ergibt, Originalunterlagen bei den Versicherten angefordert werden. Die Bearbeitung der fachlich auffälligen und der stichprobenweise geprüften Fälle sollte revisionssicher dokumentiert werden.

  Diese Regeln sind auch im Risikomanagement und IKS zu verankern.

5.2.4 Change-Management

Die Änderungen der Geschäftsprozesse der automatisierten Sachbearbeitung bergen fachlich z. T. die gleichen Risiken (Festlegung der richtigen fachlichen Parameter) sowie im organisatorisch-technischen Bereich verschiedene Risiken wie bei deren Aufbau (siehe Abschnitt

1). Daher sollten die Geschäftsprozesse zur Änderung fachlicher und technischer Parameter der Sachbearbeitung allgemein festgelegt werden. In die Änderungsverfahren sollten auch jeweils die relevanten Stellen / Fachbereiche des SV-Trägers nach einem festen Geschäftsprozess verpflichtend eingebunden werden:

- Fachbereich (materielles Recht und Fachprozesse)
- IT-Bereich
- Datenschutz
- IT-Sicherheit
- Risikomanagement und Internes Kontrollsystem
- Speicherung und Archivierung

Eine nachvollziehbare Dokumentation auch des Änderungsprozesses ist dringend zu empfehlen, damit ggf. im Nachhinein noch mögliche Fehlerquellen bzw. Verbesserungsmöglichkeiten identifizierbar sind.

5.2.5 Datenintegrität, Datensicherheit und Datenschutz

Die Integrität der in die automatisierte Sachbearbeitung eingehenden (Original-)Daten ist zu wahren, insbesondere, wenn diese als Beleg dienen sollen.
Auch die im Rahmen der Sachbearbeitung bearbeiteten Daten sind integer zu halten. Es muss dauerhaft nachvollziehbar sein, welche Änderungen der Daten durch technische wie manuelle Bearbeitungsschritte erfolgt sind.

Die Anforderungen der Datensicherheit und des Datenschutzes sind auch bei den einzelnen Verfahren der Sachbearbeitung zu erfüllen (siehe Abschnitt 1).
Die Risiken können bei Verfahren der automatisierten Sachbearbeitung höher sein, da ggf. bei Fehlern eine Vielzahl von Fällen betroffen sein kann. Daher sind diese Anforderungen sorgfältig zu betrachten.

Die revisionssichere Beständigkeit der Daten (Fachdaten, Metadaten) der automatisierten Sachbearbeitung auch bei Migration (kassenintern, Nutzung von Dienstleistungsunternehmen) ist bereits beim Aufbau von Anwendungen und spätestens vor konkreten Migrationsschritten zu beachten.
Die Anforderungen beziehen sich dabei auf alle denkbaren Schritte von Datenmigrationen, z. B.:

- bei Auslagerung der Daten in Archivsysteme
- bei Migration der Daten beim Austausch von Systemen / Anwendungen der automatisierten Sachbearbeitung
- bei Änderung von Inhouse-Formaten und Konvertierungsvorgaben.

5.2.6 Langzeitspeicherung

Nach Punkt 2.6 der Grundsätze ordnungsgemäßer Aufbewahrung gem. § 110a SGB IV[58] müssen - sofern Software zur automatisierten Sachbearbeitung eingesetzt wird - die durch

[58] Grundsätze ordnungsmäßiger Aufbewahrung im Sinne des § 110a SGB IV, Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie Aufbewahrungsfristen für Unterlagen für den Bereich der gesetzlichen Kranken- und Pflegeversicherung, Version 4.0. Siehe auch die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) des BMF, BStBl I S. 1269, abrufbar unter: https://ao.bundesfinanzministerium.de/ao/2021/Anhaenge/BMF-Schreiben-und-gleichlautende-Laendererlasse/Anhang-64/anhang-64.html

die Software durchgeführten Änderungen am Datenbestand und die diesen Prozess anstoßenden Regeln und Personen nachvollziehbar dokumentiert werden. Dies gilt ebenso für das allgemeine Regelwerk dieser Software sowie für dessen Änderungen.

Aus Sicht von Prüfungen und Revision (auch der SV-Träger) ist neben der nachvollziehbaren Dokumentation der eingeführten / geänderten Regeln und Änderungen am Datenbestand ebenso wichtig, dass diese Dokumentation revisionssicher geführt wird. Damit kann dann auch unveränderbar der jeweilige Prozess nachvollzogen werden.

Auch die sog. Meta-Informationen (Regeln, ändernden Personen und die Informationen zu Änderungen des Datenbestandes) sind an sich Daten, die wiederum Aufbewahrungsfristen unterliegen können. Die Meta-Information und deren Aufbewahrungsfrist sind dabei abhängig von den Grunddaten, auf die sie sich beziehen.

Die Anforderungen an die Speicherung gelten auch für „Massenbriefe“ bzw. Serienbriefe, bei denen vorab festgelegte Inhalte an einen definierten Personenkreis versandt werden. Systemseitig ist revisionssicher festzuhalten, welche Schreiben mit welchen Parametern (Adressatenkreis, Inhalt, in Bezug genommene Variablen, welcher Datenstand) versandt wurden. Die Verknüpfung der inhaltlichen Daten zum Personenkreis / Adressatenkreis ist ebenfalls festzuhalten.
Das dem Versicherten zugesandte Dokument muss nicht als Einzel-Datei gesondert erstellt und revisionssicher gespeichert werden. Zu empfehlen ist jedoch, dass die Sachbearbeitung im System des SV-Trägers nachvollziehen kann, welche Informationen (Personenkreis, Inhalt, Datum) den Versicherten übermittelt worden sind.

Bei sog. eAkte-Anwendungen muss der Inhalt nachvollziehbar sein.[59] Die Bearbeitungsinformationen („Meta-Informationen“) und Inhalte müssen revisionssicher gespeichert werden. Die Inhalte der eAkte-Anwendung müssen auslesbar und herstellbar sein.

Die gesetzlich vorgesehenen Aufbewahrungsfristen sind auch bei automatisierter Sachbearbeitung zu beachten. Hierzu können die Grundsätze der Aufbewahrung des GKV-Spitzenverbandes nach § 110a SGB IV (sog. Aufbewahrungskatalog) herangezogen werden.

Die Aufbewahrungsfristen beziehen sich auf folgende Daten:

- die fachlichen Daten
- die Daten der Verarbeitungsdokumentation (sog. Metadaten)

Die entsprechenden Daten sind in geeigneten Archivsystemen aufzubewahren (siehe Abschnitt 7 „Langzeitspeicherung und Löschung“).

5.3 Zahlung

5.3.1 Zahlungsfreigabe und Entwerten digitaler Belege

Durch die Änderung der SVRV und der SRVwV ist eine trägerinterne Zahlungsfreigabe in elektronischer Fassung nun nicht mehr allein durch die QES zu erreichen (siehe § 41 Abs. 1 S. 3 SRVwV). An die Stelle der QES können auch technisch-organisatorische Maßnahmen

[59] Organisationskonzept elektronische Verwaltungsarbeit, abrufbar unter: https://www.verwaltung-innovativ.de/DE/Verwaltungsdigitalisierung/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html.

treten, die die entsprechenden Risiken minimieren (§ 40 SRVwV, Anlage 9 zur SRVwV).[60] Hierfür ist eine eingehende Risikoabschätzung durch die Träger erforderlich.

Nach entsprechender Änderung der SRVwV kann für den Ersatz einer Unterschrift vorgesehen werden, dass hierfür die fortgeschrittene Signatur ausreichend ist.[61] Dies kann ermöglicht werden, da Unterschriften ausnahmslos von hierfür bestimmten Mitarbeitenden unter den Bedingungen zusätzlicher Zugangs- und Berechtigungskonzepte verbunden mit entsprechenden Kontrollen geleistet werden, die entsprechend den Anforderungen aus Anlage 9 zu gestalten und in die dortigen Verfahrensdokumentationen und Verfahren einzubeziehen sind.[62] Dies ist dann in der Risikoabschätzung der Träger einzubeziehen.
Insbesondere müssen die technischen und organisatorischen Maßnahmen sicherstellen, dass das IT-gestützte Verfahren vor unbemerkter und unberechtigter Veränderung im Sinne des § 40 SRVwV geschützt ist und das Verfahren lückenlos dokumentiert wird. Für das IT-gestützte Verfahren sind folgende Parameter zu definieren und aufeinander abzustimmen:

- Aufgaben,
- Kompetenzen, z.B.
    - Zugriffsrechte,
    - Freigabeberechtigungen mit Freigabegrenzen,
- Verantwortlichkeiten, z.B.
    - Zuständigkeit zur Einrichtung der Rollen und Berechtigungen,
    - Vorgaben zur Einrichtung, Änderung, Deaktivierung, Löschung,
    - Anwendungsfälle zum Vier-Augen-Prinzip,
- Kontrollen, z.B. Stichprobenverfahren,
- Kommunikationswege.

Die jeweils für einen Fall (Rechnung) gültige bzw. angewandte Systemeinstellung ist revisionssicher zu dokumentieren und idealerweise aus dem System heraus transparent und lückenlos nachvollziehbar (eventuell auch mit Hilfe von hinterlegten Prozessschritten). Es soll nachvollzogen werden können, welche (technisch eindeutig bestimmbaren) Mitarbeitenden des Trägers an der Prüfung und Freigabe der Rechnung beteiligt waren. Die dazugehörigen Metadaten sind entsprechend der eigentlichen Rechnung aufzubewahren und im Löschkonzept der Kasse aufzunehmen. Auch in diesem Zusammenhang geführte Korrespondenzen sind revisionssicher zu speichern.

Nach § 5 Abs. 2 SVRV ist sicherzustellen, dass eine nochmalige Verwendung von Belegen ausgeschlossen ist. Diese Anforderung des Entwertens gilt auch für digitale Belege, da diese nach § 6 Abs. 3 SVRV elektronisch erzeugte Dateien oder Datensätze Belege sein können. Dabei muss für die Entwertung dieser digitalen Belege eine im Vergleich zu Papierbelegen gleichwertige Sicherheit erreicht werden. Dies kann durch das Zusammenspiel von technischen und organisatorischen Maßnahmen erreicht werden, wobei wichtige Bausteine des Maßnahmenbündels immer an den jeweiligen Schutzbedarf angepasste Berechtigungskonzepte und Authentifizierungslösungen sowie die revisionssichere Archivierung sind. Die Darstellung des Entwertens muss in jedem Fall technisch fest mit dem jeweiligen Beleg verbunden sein.[63]

---

[60] Siehe u.a. hierzu Rundschreiben des GKV-Spitzenverbandes 2020/478 vom 24.06.2020 und das Rundschreiben des BAS vom 22.06.2020 (Az. 511 – 3700 – 1738/2007).
[61] Elfte Allgemeine Verwaltungsvorschrift zur Änderung der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung
[62] Siehe Rundschreiben des BAS vom 22.06.2020, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-78afa2ef60/
[63] Siehe Digitalausschuss des BAS, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/digitalisierung-im-rechnungswesen/entwerten-digitaler-belege/

5.3.2 Digitalisierung bei Abrechnungs- und Verordnungsprüfung

Voraussetzung der Digitalisierung von Originalbelegen ist zunächst die Einhaltung der Anforderungen an (Scan-)Verfahren (siehe Abschnitt 3). Daneben müssen die Träger in der Lage sein, die Anforderungen an die Schutzziele „Integrität“, „Vertraulichkeit“ und „Verfügbarkeit“ zumindest nachvollziehen zu können. Sollten die Originalbelege dabei nicht im unmittelbaren Zugriffsbereich der Krankenkassen vorliegen (zur Speicherung des Originaldatensatzes siehe Punkt 6.2), so müssen die aus diesen Originalbelegen hervorgehenden Datensätze im Sinne der allgemeinen Anforderungen erstellt worden sein und die Datensätze den Trägern mit einem sicheren Integritätsschutz (z.B. mit QES oder Sicherungsmittel mit gleicher Schutzstärke) verschlüsselt übermittelt werden.

5.3.3 Externe Zahlungsdienste

Der Einsatz von externen Zahlungsdienstleistern ist nur unter besonderen Bedingungen möglich:[64] :

- Wirtschaftlichkeit des Einsatzes dieser Instrumente,
- Einhaltung der Regelungen des Datenschutzes,
- entsprechende Berücksichtigung der vermögensrechtlichen Vorgaben des SGB IV.

5.3.4 Ersetzendes Scannen bei Abrechnungsprüfung

Die Aufbewahrung von Papieroriginalen insbesondere im Rahmen der Abrechnung von Leistungserbringung erfordert einen hohen Aufwand. Aus diesem Grund ist das „ersetzende Scannen“ von Originalverordnungen für die sonstigen Leistungserbringer nach § 302 SGB V als auch die Krankenkassen von hoher Bedeutung.
Bei der Betrachtung der Möglichkeiten und Folgen des ersetzenden Scannens sind das Abrechnungsverfahren und das Abrechnungsprüfverfahren als getrennte Verfahren zu unterscheiden.
Es bestehen zwei grundsätzliche Möglichkeiten, im Rahmen der Abrechnungs- und des Abrechnungsprüfungsverfahren Scandokumente von Abrechnungsformularen der Leistungserbringer als Grundlage und Belege zu Grunde zu legen, die nachfolgend dargestellt und bewertet werden.

5.3.4.1 Ersetzendes Scannen in der Sphäre der Krankenkassen

Ein elektronischer Beleg und damit eine rechtssichere Grundlage für die Abrechnungsprüfung wird (erst) in der Sphäre der Krankenkasse erstellt. Dies kann durch die Krankenkasse oder ein durch sie für den Scanprozess beauftragtes Dienstleistungsunternehmen erfolgen. Die Abrechnungsprüfung erfolgt dann auf der Grundlage dieses elektronischen Beleges.

Zur Einleitung der Abrechnung (Abrechnungsverfahren) kann jedoch – z.B. im Vorfeld der Abrechnungsprüfung – auf Scandokumente aufgesetzt werden, die auch in der Sphäre der Leistungserbringer erstellt werden können. Dabei wird dann in dieser Sphäre nicht ersetzend gescannt, so dass auf die Anbringung einer qualifizierten elektronischen Signatur verzichtet werden muss, um nicht bereits an dieser Stelle ein das Original ersetzendes elektronisches Dokument zu erstellen. Ein das Original ersetzendes elektronisches Scanprodukt erfolgt

[64] Bestandsaufnahme des Digitalausschuss im BAS (Stand 30.06.2020).

dann wie – wie oben dargestellt – (erst) durch das Scanverfahren in der Sphäre der Krankenkasse.

Auf der Basis dieser das Original nicht ersetzenden Scandokumente (Sphäre Leistungserbringer) kann dann in der Sphäre der Krankenkassen (Krankenkasse bzw. Abrechnungsdienstleistungsunternehmen der Krankenkassen) bereits die Abrechnung der Leistungserbringer erfolgen.
Die Originalabrechnungsformulare (Papier) sind dann an die Krankenkassen bzw. deren Dienstleistungsunternehmen (für Scanprozess) zu leiten, bei denen dann, wie im ersten Absatz ausgeführt, das ersetzende Scannen vorgenommen werden kann. Auf diesen das Original ersetzenden Scandokumenten setzt dann die Abrechnungsprüfung in der Krankenkassensphäre (Krankenkasse bzw. deren Dienstleistungsunternehmen der Abrechnungsprüfung) auf.

5.3.4.2 Ersetzendes Scannen in der Sphäre der Leistungserbringer

Theoretisch ist auch ein ersetzendes Scannen der Abrechnungsbelege in der Sphäre der Leistungserbringer möglich.

Bei einem ersetzenden Scannen (Aufbringung einer qualifizierten elektronischen Signatur) in dieser Sphäre würde dann das elektronische Scandokument das (einzige) Original darstellen und Belegwirkung auch für die Abrechnungsprüfung in der Sphäre der Krankenkasse entfalten. Diese „Originalität“ ergibt sich aus dem Rechtsgedanken des § EGovG, der den vormaligen § 110d SGB IV insoweit ersetzt. Eine Weiterleitung der Papierfassung und nochmaliges ersetzendes Scannen in der Sphäre der Krankenkasse wären dann nicht mehr erforderlich und rechtlich auch nicht möglich, da ansonsten zwei elektronische „Originaldokumente“ bestehen würden.

Diese Alternative ist an weitere Anforderungen gebunden, um die Dokumente als Abrechnungsbelege qualifizieren zu können.

So bindet der Beschluss unter TOP 20 der 102. Aufsichtsbehördentagung die Anerkennung der in der Sphäre der Leistungserbringer erzeugten Images aus ersetzendem Scannen an die Anforderung, dass zum Zweck der Überprüfung der Papierbelege diese für die Kassen erreichbar sein müssen.[65] Um die Anforderungen an eine Anerkennung der durch die

Leistungserbringer erzeugten Images als Belege konkreter zu fassen, können die folgenden Punkte als Grundlage der Beratung seitens der Prüfdienste herangezogen werden:

- Es ist seitens der Krankenkassen eine gesonderte Risikobetrachtung eines solchen Verfahrens vorzunehmen. Zwar muss auch der ersetzende Scanprozess, der dann in die Sphäre der Leistungserbringer verlagert ist, nach den gesetzlichen Anforderungen (umgesetzt in der TR-RESISCAN) erfolgen. Allerdings besteht an dieser Stelle die Besonderheit, dass die ersetzend scannende Stelle nicht neutral ist und dort insbesondere im Abrechnungsprüfverfahren eigene Interessen verfolgt werden. Dies macht eine Risikobetrachtung erforderlich.
- Aus dieser Risikobetrachtung müssen Maßnahmen erwachsen, die mögliche Risiken (d.h. Möglichkeiten zu Fehlabrechnungen zu Lasten der Krankenkassen) bis zu einem aus Sicht der Krankenkassen vertretbaren Niveau minimieren.

[65] Abrufbar unter: https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Aufsichtsbehoerdentagung/20230609Protokoll_102_AT.pdf

- Die konkreten Verfahren der Scandienstleister der Leistungserbringer sollten hierzu bewertet und ggf. auf die Umsetzung der Konzeption im tatsächlichen Scanverfahren aus der Sphäre der Kasse heraus geprüft werden.
- Ergänzend wäre aus unserer Sicht auch das Recht der Krankenkassen gegenüber den Leistungserbringern zu vereinbaren, in einem bestimmten Zeitraum nach dem ersetzenden Scannen und der Übermittlung der elektronischen Belege in die Sphäre der Krankenkassen (Krankenkassen bzw. deren Abrechnungsdienstleistungsunternehmen) nicht nur in Fällen möglicherweise technisch nicht sauberer bzw. nicht eindeutig lesbarer Fälle, sondern in einem zu bestimmenden Umfang stichprobenweise Papieroriginale zu Scandokumenten anzufordern. Diese Papierfassungen können dann in der Sphäre der Krankenkassen mit dem Scandokument abgeglichen werden.

  Alternativ können diese Überprüfungen auch während des laufenden Sachbearbeitungsprozesses innerhalb der SV-Träger erfolgen, wenn auch hierbei eine ausreichende Zahl an Images überprüft wird.

- Die Höhe der Stichproben sollte wiederum risikoorientiert festgelegt werden. Parameter hierfür könnten z.B. sein:
  - Gesamtzahl der übermittelten elektronischen Belege,
  - Bei Beginn des Verfahrens höhere Stichprobe und dann ggf. Anpassung in Abhängigkeit von gewonnenen Erkenntnissen,
  - Schichtung der Stichprobe nach inhaltlichen Kriterien, die besondere Fälle erfassen kann (z.B. hochpreisige Leistungen) aber auch einen Durchschnitt der Fälle (z.B. Scans von verschiedenen Tagen, Höhe der Kosten der Leistung) etc.
- Das Verfahren und die Erkenntnisse aus den Stichprobenprüfungen sollte dokumentiert werden, so dass ggf. eine Anpassung des Verfahrens erfolgen kann.

6 Elektronischer Datenaustausch

Der Austausch von Daten zwischen SV-Trägern, mit anderen öffentlichen Stellen und Dritten erfolgt weitgehend elektronisch.

Um die Datenintegrität nachzuweisen, sind die im § 110a Abs. 1 SGB IV gestellten Anforderungen zu beachten. Danach sind Unterlagen, die für die öffentlich-rechtliche Verwaltungstätigkeit, insbesondere für die Durchführung eines Verwaltungsverfahrens oder für die Feststellung einer Leistung, erforderlich sind, nach den Grundsätzen ordnungsmäßiger Aufbewahrung[66] sicher zu speichern. Zu den „Unterlagen“ in diesem Sinne gehören auch Daten, die nur mit Hilfe einer Datenverarbeitungsanlage erstellt worden sind.

Daraus folgt, dass die SV-Träger bei der Annahme elektronischer Datensätze den Originaldatensatz im Sinne der Aufbewahrungspflichten nach § 110a SGB IV dauerhaft und unveränderbar entsprechend der jeweils geltenden Aufbewahrungsfrist zu speichern haben. Auf die Ausführungen zu den Aufbewahrungsfristen wird auf Ziffer 7.3.1 verwiesen. Hierzu sind geeignete Archivsysteme zu nutzen, die eine Versionsintegrität gewährleisten (siehe hierzu Ausführungen zu nicht wieder beschreibbaren Datenträgern unter Punkt 3.2.3). Der SV-Träger muss im Zweifelsfall den Nachweis erbringen, dass die Ursprungsdatensätze im Original vorliegen und nicht verändert wurden[67].

Die Daten müssen für Revisionszwecke zeitnah zur Verfügung stehen.

Die Auftragsdaten (Vorlaufdatensatz) und die Nutzdaten sind nach Eingang beim SV-Träger (oder beauftragten Dritten) direkt nach der Entschlüsselung elektronisch zu speichern. Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (z. B. EDIFACT, XML, JSON) in eine lesbare Form umzuwandeln.
Werden die Daten nach der Speicherung des Original-Datensatzes in den operativen DV-Systemen verarbeitet, sind die vorgenommenen Datenänderungen in den Fachverfahren im Sinne einer Historienführung nachvollziehbar zu protokollieren.

6.1 Ergänzende rechtliche Grundlagen

§ 78 SGB IV bildet die Rechtsgrundlage, Grundsätze u. a. für die Zahlung, die Buchführung und die Rechnungslegung festzulegen. Die Regelung ist nach den Grundsätzen des für den Bund und die Länder geltenden Haushaltsrechts vorzunehmen und hat die Besonderheiten der SV-Träger und der einzelnen Versicherungszweige zu berücksichtigen.
Aufgrund der Regelungskompetenz nach § 78 SGB IV wurden die Grundsätze des Rechnungswesens in der SVRV und Detailregelungen in der SRVwV festgelegt. Ergänzend hat der GKV-Spitzenverband in Zusammenarbeit mit der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherungen GmbH (ITSG) insbesondere „Gemeinsame Grundsätze Technik für die elektronische Datenübermittlung gem. § 95 SGB IV“ erarbeitet.[68] Die Dokumente regeln detailliert die technischen Vorgaben der Datenfernübertragung und dem Datenträgeraustausch zwischen Arbeitgebern bzw. Leistungserbringern und SV-Trägern. Sie sind für die Beteiligten verbindlich.

Auch trägerübergreifender Datenaustausch ist bei Vorliegen entsprechender Tatbestände möglich (z. B. § 197 a Abs. 3a SGB V).

---

[66] § 110c SGB IV bzw. Heranziehung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).
[67] Rundschreiben GKV-Spitzenverband Nr. 179/2022 vom 21.03.2022 mit Anlage, Ziffer 2.7 der Anlage
[68] Abrufbar unter: www.gkv-datenaustausch.de

6.2 Speicherung des Originaldatensatzes

Bei elektronischen Eingängen sind entsprechende Vorschriften zur Aufbewahrung der Daten zu erfüllen. In der Sozialversicherung sind dies Art. 5 und Art. 32 DSGVO, § 67b Abs. 1 S. 4 SGB X i. V. m. § 22 Abs. 2 BDSG, die SVHV sowie die SVRV i. V. m. der SRVwV.

§ 6 Abs. 3 SVRV stellt klar, dass Belege auch elektronisch erzeugte Dateien oder Datensätze sein können. Somit ist sichergestellt, dass die rechtlichen Anforderungen für Belege auch für elektronische Datensätze gelten.

Die Anforderungen von § 9 Abs.1 und 3 SRVwV zur Belegführung und § 12 Abs. 2 SRVwV zu zuzahlungsbegründenden Unterlagen sind zu beachten.

Es muss eine Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv gegeben sein.

Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (EDIFACT; XML, JSON) in eine lesbare Form umzuwandeln.

6.3 Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung)

Automatisierte Verfahren sind durch geeignete technische und organisatorische Maßnahmen vor unbemerkter und unberechtigter Veränderung zu schützen. Die zur Sicherheit dieser Verfahren zu erlassende Dienstanweisung muss die in Art. 5 und Art. 32 DSGVO, § 67b Abs. 1 S. 4 SGB X i. V. m. § 22 Abs. 2 BDSG erforderlichen technisch-organisatorischen Maßnahmen regeln. Insbesondere ist darauf hinzuweisen, dass Einzelheiten von Verfahrensänderungen und neu eingeführter Verfahren entsprechend der Anlage 9 zu § 40 SRVwV zu dokumentieren sind. Mit dieser Regelung wird der Einsatz moderner IT-Technik im Rechnungswesen berücksichtigt und die Prüfbarkeit von Abrechnungsverfahren (Verfahrens- und Systemprüfungen) sichergestellt. Aus der Dokumentation muss sich ergeben, dass das Verfahren entsprechend seiner Beschreibung durchgeführt worden ist.

Das gesamte Verfahren ist in einer ausführlichen Verfahrensbeschreibung darzustellen. Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind. Tabellen, über die die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln. Änderungen von Tabellen mit Programmfunktion sind in der Weise zu dokumentieren, dass für die Dauer der Aufbewahrungsfrist der jeweilige Inhalt einer Tabelle festgestellt werden kann.

In einer Gefährdungsanalyse sind die Risiken zu ermitteln und zu bewerten. Die Einführung und die wesentliche Änderung eines IT-gestützten Verfahrens sind nur zulässig, sofern Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können. Somit sind automatisierte Verfahren durch Regelungen von technischen und organisatorischen Maßnahmen vor unbemerkten und unberechtigten Veränderungen zu schützen. Die Anwendungen haben sicherzustellen, dass dokumentiert wird, wer zu welcher Zeit Änderungen an den Daten vorgenommen hat. Verfahrensänderungen sind so zu dokumentieren, dass die Prüfbarkeit des Abrechnungsverfahrens für einen sachverständigen Dritten darstellbar und nachvollziehbar sichergestellt ist.

6.4 Dokumentation und Prüfbarkeit der Buchführung

Nach den Vorschriften der SVRV sind die Grundsätze ordnungsmäßiger Buchführung zu beachten. Bei der Nutzung von IT-Verfahren sind die Sicherheitsanforderungen in einer Dienstanweisung (siehe § 40 SRVwV) zu bestimmen und zu dokumentieren. Auch bei fremderworbener Software, bei der Teile der Verfahrensdokumentation vom Softwarehersteller angefertigt werden, ist der Buchführungspflichtige für die Vollständigkeit, Nachvollziehbarkeit und den Informationsgehalt der Verfahrensdokumentation verantwortlich.

Die Verfahrensdokumentation der Software muss den Anforderungen der Anlage 9 zu § 40 SRVwV genügen.

6.5 Interoperabilität

Das von der Gesellschaft für Telematik (gematik) gem. Art. 1 Patienten-Datenschutz-Gesetz (PDSG) in Verbindung mit § 385 SGB V festgelegte Interoperabilitätsverzeichnis fördert die Interoperabilität zwischen informationstechnischen Systemen im Gesundheitswesen. Dabei soll im Sinne einer sinnvollen Nutzung ein übergeordneter Zweck des Datenaustausches impliziert sein.[69]

Die Anforderung eines möglichen Datenaustausches bzw. dessen technische Ermöglichung ist bei der Gestaltung der Systeme der Träger des Gesundheitswesens zu beachten.

6.6 Meldeverfahren EESSI

Die Anforderungen bzw. Schnittstellen für eine Anbindung des Systems des SV-Trägers im Hinblick auf den „Elektronischen Austausch von Sozialversicherungsdaten“ (EESSI) sind im Bereich des Datenaustausches (siehe Punkt 4.4.2) mit den EU- und EFTA-Staaten zu beachten. Die Abwicklung erfolgt insbesondere durch die zuständigen Verbindungsstellen der SV-Träger (z. B. DVKA).

6.7 Verfahren nach § 79 SGB X

Die technischen und verfahrensmäßigen Anforderungen an die automatisierten Verfahren zum Datenabruf (insbesondere nach Abs. 2: Einrichtung automatisierter Verfahren auf Abruf) sind bei der Gestaltung dieser Verfahren zu berücksichtigen.

[69] Siehe Unterrichtung durch die Bundesregierung vom 12. Januar 2018, BT-Drs. 19 / 451, S. 2.

7 Langzeitspeicherung und Löschung elektronisch erzeugter Dokumente und Daten

7.1 Langzeitspeicherung

Grundsätzlich sind alle elektronisch vom SV-Träger erzeugten oder von Versicherten bzw. Dritten übermittelten elektronischen Dokumente, die für den jeweiligen Bearbeitungsvorgang oder das „Versicherungsleben“ einer versicherten Person rechtserheblichen Charakter („Beweischarakter“) haben, in einem elektronischen Langzeitarchiv revisionssicher aufzubewahren.

Eingehende Dokumente

Dazu zählen insbesondere:

- Elektronisch erzeugte Dokumente (z. B. im DOCX-, PDF- oder XML-Format), die elektronisch an den SV-Träger übermittelt wurden (z. B. über Datenträger, E-Mail, Upload-Portale oder sichere Übertragungsdienste),
- Eingegangene elektronische Faxe oder digital übermittelte Faxkopien,
- Eingegangene E-Mails, und deren Anhänge,
- Über Online-Formulare auf der Internetseite des SV-Trägers erzeugte und übermittelte Daten (Text- oder PDF-Format).

Ausgehende / erzeugte Dokumente

Dazu zählen insbesondere:

- „Durchschriften“ der vom SV-Träger (einschließlich seiner Beschäftigten) elektronisch erzeugten und an externe Empfänger versandten Dokumente sowohl in elektronischer als auch in Papierform),
- Vom SV-Träger an Externe (z. B. Versicherte, Arbeitgeber, Leistungserbringer) versandte E-Mails, sowie deren Anhänge,
- Interne Vermerke, Verfügungen, Notizen und Protokolle, soweit diese für den Vorgang rechtlich oder fachlich bedeutsam sind.

Die Anforderungen an eine rechtssichere und elektronische Langzeitspeicherung ergeben sich aus:

- den §§ 110a – 110c SGB IV i. V. m. den Grundsätzen ordnungsgemäßer Aufbewahrung,
- dem EGovG sowie ergänzend dem OZG,
- den Vorgaben zur Sicherheit der Verarbeitung gem. Art. 32 DSGVO,
- den technischen und organisatorischen Vorgaben nach § 67b Abs. 1 S. 4 SGB X i. V. m. § 22 Abs. 2 BDSG.

Weiterhin sind die vom Verband Organisations- und Informationssysteme e. V. (VOI) aufgestellten Merksätze zur revisionssicheren elektronischen Archivierung zu beachten:

- Jedes Dokument ist unveränderbar aufzubewahren.
- Kein Dokument darf auf dem Weg ins oder im Archiv verloren gehen.
- Jedes Dokument muss mit geeigneten Such- oder Retrievaltechniken eindeutig auffindbar sein.
- Es muss eindeutig dasjenige Dokument wiedergefunden werden, das gesucht wird.
- Während der vorgesehenen Aufbewahrungszeit darf kein Dokument gelöscht oder zerstört werden.

- Dokumente müssen in exakt der Form angezeigt und ausgegeben werden, in der sie erfasst wurden.
- Der Zugriff auf Dokumente muss zeitnah und nachvollziehbar möglich sein.
- Änderungen an Organisation oder Struktur des Archivs sind vollständig zu protokollieren, sodass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Archive sind so auszugestalten, dass eine Migration auf neue Plattformen, Medien, Softwareversionen oder Komponenten ohne Informationsverlust möglich ist.
- Das Archivsystem muss gewährleisten, dass sämtliche gesetzliche und interne Bestimmungen zur Datensicherheit und zum Datenschutz über die Lebensdauer des Archivs eingehalten werden.

7.2 Langfristige Beweiserhaltung nach § 15 VDG

Neusignierung von elektronischen Signaturen:
Elektronische Signaturen basieren auf mathematischen Verschlüsselungsverfahren. Der technische Fortschritt führt dazu, dass Signaturalgorithmen nach einem bestimmten Zeitablauf nicht mehr als sicher angesehen werden können.
Die Sicherheits- und Beweiseignung der elektronischen Signatur ist zeitlich begrenzt, wenn nicht weitergehende Maßnahmen ergriffen werden. Insbesondere bei der Langzeitspeicherung in Archiven kommt dieser Fall häufig vor.
Mit § 15 VDG hat der Gesetzgeber hierfür eine entsprechende Regelung geschaffen: „Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen.“
Für die Erzeugung der elektronischen Signaturen sind die Vorgaben der SOG-IS Agreed Cryptographic Mechanisms[70] und der BSI TR-02102 einzuhalten.

Die erneute Signatur mit neuen Algorithmen und zugehörigen Parametern muss zu einem Zeitpunkt erfolgen, in dem die alte Signatur noch sicher ist. Um zu beweisen, dass dieses sog. Übersignieren rechtzeitig erfolgt ist, muss ein qualifizierter Zeitstempel angebracht werden. Wird dieses Verfahren regelmäßig angewendet, kann der Beweiswert und die Beweiseignung einer elektronischen Signatur noch nachgewiesen werden, auch wenn die Ursprungssignatur alleine zwischenzeitlich unsicher geworden ist.

Neusignierung von Hashalgorithmen:
Genauso wie bei der erstmaligen Signatur geht es bei der Neusignatur auch darum, sie effektiv und kostengünstig durchzuführen. Das Übersignieren soll handhabbar sein und die Anzahl der notwendigen Zeitstempel geringgehalten werden.

Auch bei der Neusignatur wird nicht das Dokument selbst, sondern der Hashwert signiert.

Wird ein Hashalgorithmus ab einem bestimmten Zeitpunkt nicht mehr als sicher eingestuft, so gelten auch hier die Bestimmungen nach § 15 VDG; d. h., es ist ein neuer Hashwert mit einem als sicher beurteilten Verfahren (für jedes Dokument) zu bilden, mit einer qualifizierten Signatur (neue Signaturalgorithmen und Parameter) zu signieren und ein qualifizierter Zeitstempel anzubringen.

Neusignierung von Zeitstempeln:
Sollte der qualifizierte Zeitstempel, sofern er selber auf einer qualifizierten Signatur beruht, als unsicher eingestuft werden, reicht es aus, den Hashwert über die archivierten Dokumente

[70] Abrufbar unter https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

zu erzeugen, alle früheren Signaturen dabei mit einzuschließen und dann einen solchen sog. kryptografischen Zeitstempel (qualifizierte Zeitstempel der auf einer aktuellen qualifizierten Signatur beruht) für diesen Hashwert einzuholen.

Vorausgesetzt, die Signatur, die der Zeitstempel trägt, basiert auf den neuen Algorithmen und Parametern, entfällt in diesem Fall die Notwendigkeit, nochmals eine eigene qualifizierte Signatur anzubringen.

Um eine Beweiswirkung zu erhalten, haben die SV-Träger rechtzeitig eine Nachsignatur zu veranlassen.

Nehmen SV-Träger die Nachsignatur erst nach dem Ablauf vor, fällt der Vorteil des Anscheinsbeweises (Privileg des Beweises des ersten Anscheins) weg. Für den SV-Träger tritt im Streitfall die Umkehr der Beweislast ein.

Die Archivlösung sollte die verschiedenen Verfahren zur Neusignierung beherrschen.

7.3 Besonderheiten

7.3.1 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen

Für die in einer elektronischen Akte (eAkte) aufzubewahrenden Einzeldokumente können gem. Aufbewahrungskatalog unterschiedliche Aufbewahrungsfristen gelten[71].. In diesem Fall richtet sich der Endzeitpunkt der Aufbewahrungspflicht der Fallakte nach dem in ihr enthaltenen Einzeldokument mit der längsten Aufbewahrungsdauer. Diese „Verlängerung“ der Aufbewahrung verstößt nicht gegen das Löschgebot aus § 84 Abs. 2 S. 2 SGB X, da die Fallakte einen Gesamtzusammenhang schafft, in dem eine Aufbewahrung zur allgemeinen Aufgabenerfüllung des SV-Trägers erforderlich sein kann. Bei elektronisch gespeichertem Schriftgut sind die Vollständigkeit, Integrität, Authentizität und Lesbarkeit durch geeignete Maßnahmen zu gewährleisten[72].

Es gibt unterschiedliche Ausprägungen elektronischer Vorgangsbearbeitungen, dennoch wird dringend empfohlen, eine zeitnahe und vollständige Umstellung auf elektronische Akten und auf eine digitale Bearbeitung anzustreben[73]. Auf diese Weise können die Prinzipien der Datenminimierung und ggf. Auskunftsansprüche von Betroffenen praktisch wirksam und effizient umgesetzt werden. Die Archivlösung der SV–Träger kann gegen die in der TR-ESOR aufgeführten Anforderungen und deren Konformität festgestellt werden (s. Punkt 4.3.3).

7.4 Löschung von Daten der elektronischen Kommunikation

Die Verpflichtung zur Löschung personenbezogener Daten ergibt sich aus Art. 17 Abs. 1 DSGVO. Die Umsetzung dieser Vorgabe erfordert bei zunehmendem Komplexitätsgrad ein detailliertes Löschkonzept[74]. Zudem müssen in einem Verfahrensverzeichnis gem. Art. 30 Abs. 1 S. 2 Buchst. f DSGVO die entsprechenden Löschfristen spezifiziert werden.

Bei der Erstellung des Löschkonzeptes und der Löschfristen ist zu beachten, dass hierunter

[71] Aktualisierung der Grundsätze ordnungsgemäßer Aufbewahrung, Rundschreiben GKV-Spitzenverband Nr. 179/2022 vom 21.03.2022 mit Anlage
[72] https://www.bundestag.de/resource/blob/890530/WD-6-014-22-pdf.pdf
[73] Zu Finanzämtern siehe Tätigkeitsbericht 2022 BfDI, S. 90
[74] Vorgaben zur Erstellung und den Inhalten eines Löschkonzeptes enthält die ISO /IEC 27555).

nicht nur Nutzdaten sondern auch Metadaten (z. B. Log-Daten zu Web-Seiten, Tracking-Daten und App-Nutzungsdaten) fallen.

Es wird empfohlen, die für die elektronische Kommunikation geltenden Löschregeln in das Gesamtkonzept des SV-Trägers zur Löschung von Daten aufzunehmen.

7.5 Datenspeicherung in der Cloud

Cloud Computing kann neben der eigentlichen Speicherung von Daten auch die Grundlage vieler Anwendungen sein, die aufgrund ihres besonderen Datenspeicherbedarfs bei der technischen Verarbeitung Elemente der Cloudspeicherung integriert haben (z.B. Anwendungen zur Bereitstellung von Inhalten – Content Delivery / Distribution Networks, Anwendungen des Maschinellen Lernens und der Künstlichen Intelligenz).

Für den Betrieb von Cloud Computing sind besondere datenschutzrechtliche Anforderungen zu beachten.

In jedem Fall ist für Cloud Computing eine umfassende Risikoanalyse erforderlich, dazu gehören, insbesondere wenn Gesundheitsdaten verarbeitet werden sollen, eine datenschutzrechtliche Betrachtung mit einer Datenschutzfolgenabschätzung (Art. 35 DSGVO) und die Einbindung in die Sicherheitskonzeption des SV-Trägers bzw. ein eigenständiges Sicherheitskonzept.

Private Cloud
Es muss ein wirtschaftlicher Betrieb sichergestellt sein. Bei grundlegenden Änderungen des Systemkonzepts ist eine Anzeige nach § 85 SGB IV erforderlich.

Externe Cloud im Rahmen einer Auftragsverarbeitung[75]
Bei einer Auftragsverarbeitung müssen die §§ 80 SGB X und 85 SGB IV sowie Art. 28 DSGVO beachtet werden.

Eine Auftragsverarbeitung bedarf gesonderter vertraglicher Regelungen.
Wir empfehlen, auf Vorlagen des vdek e. V. bzw. des GKV-Spitzenverbandes zurückzugreifen.
Ein bloßer Verweis auf Allgemeine Geschäftsbedingungen genügt den gesetzlichen Anforderungen nicht.

In jedem Fall sollten technische und organisatorische Maßnahmen in der Risikoanalyse aufgenommen und bewertet werden, die neben der eigentlichen Speicherung eine weitere Datenübermittlung bzw. Verarbeitung durch den Anbieter oder weitere Dienstleister (insbesondere in unsicheren Drittstaaten, s.u.) ausschließt. Zu nennen sind an dieser Stelle die verschlüsselte Übertragung (immer erforderlich) und die verschlüsselte Speicherung (Schlüssel nur beim Verantwortlichen) sowie die Nutzung sog. Souveräner Clouds.[76]
Im Rahmen des Vergabeverfahrens sollten diese Anforderungen bereits für die Ausschreibung berücksichtigt werden.

Die Wirtschaftlichkeit des Betriebs sollte durch regelmäßige Erfolgskontrollen nachgewiesen werden. Um nicht in eine Abhängigkeit zum Anbieter zu geraten, ist bei Vertragsschluss eine

[75] Abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/ki-big-data-cloud-computing-und-automatisierte-bearbeitung/cloud-computing/
[76] Zur Nutzung Souveräner Clouds s. Stellungnahme der Konferenz der unabhängigen Datenschutzbehörden (DSK) v. 11.05.2023 zu „Kriterien für Souveräne Clouds“.

Wechselmöglichkeit zu einem anderen Anbieter oder Rückmigration auf eigene Infrastruktur („Exit-Strategie“) zu vereinbaren.

Auch bei Datenübermittlung zu (Unter-)Auftragnehmern in andere Staaten sind die Vorgaben des § 80 Abs. 2 SGB X einzuhalten. Werden z.B. für Wartungs- und Servicedienstleistungen außerhalb der Beschränkungen des § 80 Abs. 2 SGB X Zugänge ermöglicht, ist eine Auftragsverarbeitung von Sozialdaten grundsätzlich unzulässig.

Sind Unternehmen, mit denen zur Cloud-Speicherung eine Auftragsverarbeitung vereinbart wird, in der EU oder in einem gleich gestellten Staat ansässig (auch als Tochterunternehmen z.B. eines in den USA ansässigen Mutterunternehmens), gelten diese als Unternehmen im Sinne des § 80 Abs. 2 SGB X. Ein Ausschluss dieser Tochterunternehmen im Rahmen eines Vergabeverfahrens nur aufgrund dieser gesellschaftsrechtlichen Stellung ist nicht möglich.[77] Der Ausschluss des weiteren Datentransfers in Staaten, die den Anforderungen des § 80 Abs. 2 SGB X nicht entsprechen, muss vielmehr in die Ausschreibeanforderungen aufgenommen werden.

Der Datenaustausch personenbezogener Daten mit den USA ist aufgrund des Angemessenheitsbeschlusses der Europäischen Kommission auf der Grundlage des „EU-US Data Privacy Framework“ und der Bestätigung durch das EuGH-Urteil von 2025 wieder möglich. Dies gilt für den Datenaustausch mit Unternehmen, die sich entsprechend dem Framework zertifizieren und in die Liste des US-amerikanischen Wirtschaftsministeriums aufnehmen lassen.[78]

Die US-Anbieter von Cloud-Dienstleistungen (sog. Hyperscaler) verfolgen zumindest für einige Verarbeitungsschritte bzw. -kategorien das sog. Follow-the-Sun-Prinzip, bei dem eine weltweite Verarbeitung der Daten (z.B. Zugriffe zur Sicherstellung der vertraglichen Serviceziele) nicht ausgeschlossen werden kann. In diesen Fällen sollten bereits in den Ausschreibungsverfahren Anforderungen aufgenommen werden, die eine Verarbeitung in „unsicheren Drittstaaten“ (keine Staaten nach § 80 Abs. 2 SGB X) ausschließen bzw. zumindest ausreichende Schutzmaßnahmen vorsehen, die einen Zugriff aus diesen Drittstaaten heraus technisch ausschließen (z.B. Verschlüsselungskonzepte, s.o. allgemeine Anforderungen).

Nach § 393 SGB V gelten im Gesundheitswesen besondere technische und organisatorische Anforderungen an die Nutzung von Clouddiensten. Diese Anforderungen sind vorrangig gegenüber den vorstehend genannten Anforderungen für andere Träger der Sozialversicherung nach allgemeinem Recht, und stellen also eine Spezifizierung des § 80 SGB X und Art. 28 DSGVO dar. Die Anforderungen einer Nutzung von Systemen nach C5-Basiskriterien legen auch im Zusammenspiel mit § 392 SGB V insoweit den Stand der Technik fest. Einschränkend gegenüber den allgemeinen Anforderungen muss ein zu wählender Cloud-Dienstleister eine Niederlassung im Inland haben.
Die Anforderungen des § 393 SGB V gelten nach dem Wortlaut und systematischer Auslegung für Auftragsverarbeiter und auch für den verantwortlichen Auftraggeber, da auf die „datenverarbeitende Stelle“ Bezug genommen wird.[79]
Für die weiteren Träger der Sozialversicherung gelten jedoch die o.g. genannten allgemeinen Anforderungen, auch an die Übermittlung an Dienstleister mit Sitz im Ausland. Die für Krankenkassen vorgesehenen technischen Anforderungen können jedoch als Möglichkeiten im Rahmen einer Risikofolgenabschätzung und Überprüfung der Wirtschaftlichkeit herangezogen werden.

[77] Bundeskartellamt 2. Vergabekammer des Bundes vom 13.02.2023, Az. VK2-114/22.

[78] Siehe Anwendungshinweise DSK vom 04.09.2023 Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

[79] BT-Drs. 20/9788, S. 207; Weichert, SGB 2024, 406, 408.

Zur Nutzung des Cloud-Dienstes Microsoft 365 (MS365) wird auf die Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) verwiesen. Laut DSK (Stand 2022, bestätigt 2025) kann der Nachweis einer vollständig datenschutzkonformen Nutzung auf Basis „Datenschutznachtrags vom 15. September 2022“ allein nicht erbracht werden[80]. Dessen ungeachtet obliegt es den öffentlichen und nicht-öffentlichen Stellen, die MS365 einsetzen, vor dem Hintergrund ihrer datenschutzrechtlichen Pflichten als Verantwortliche, alle ihnen zur Verfügung stehenden Möglichkeiten zu nutzen, auf datenschutzkonforme Vereinbarungen mit Microsoft hinzuwirken und eine datenschutzkonforme Nutzung zu ermöglichen.[81] Zudem gibt es Maßnahmen, die von den öffentlichen und nicht-öffentlichen Stellen unabhängig von vertraglichen Vereinbarungen mit Microsoft getroffen werden können, um den Datenschutz beim Einsatz von MS365 zu verbessern.[82]

[80] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

[81] Abrufbar unter: https://lfd.niedersachsen.de/download/199434&ved=2ahU-KEwii9OfM5_uGAxU37wIHHSr0AGUQFnoECBYQAQ&usg=AOvVaw0vY6P1YoQD7oo89Tf-afv1

[82] Abrufbar unter: https://www.lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung_nach_art_28_ds_gvo/handreichung-zur-auftragsverarbeitungs-vereinbarung-fur-microsoft-365-225721.html;
Der hessische Beauftragte für Datenschutz und Informationsfreiheit; hbdi_bericht_m365_2025_11_15.pdf

8 Onlineplattformen

Für die Telematikinfrastruktur als zentrale Plattform für digitale Anwendungen im Gesundheitswesen wurden die rechtlichen Rahmenbedingungen im Elften Kapitel des SGB V definiert.

Ergänzend dazu sind Digitale Gesundheitsanwendungen (DiGA) sowie Digitale Verwaltungsleistungen durch die Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) bzw. das OZG in den Fokus der SV-Träger gelangt. Beim OZG sind bisherige Verwaltungsprozesse sukzessive auch digital über Verwaltungsportale von Bund und Ländern anzubieten.

Einzubeziehen sind insbesondere:

- Gesundheits-IT-Interoperabilitäts-Governance-Verordnung (GIGV)
- Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG)
- Patientendaten-Schutz-Gesetz (PDSG)
- TR des BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen inklusive Anlagen Teile 1, 2 und 3
- Rundschreiben des BAS (siehe Fußnote 45)

8.1 Telematikinfrastruktur (TI)

Die TI dient der sicheren digitalen Vernetzung und Kommunikation aller Beteiligten. Sie ist insbesondere für die Nutzung der eGK inklusive der verpflichtenden Anwendungen der TI, wie dem Versichertenstammdatendienst, erforderlich. Daneben werden weitere Anwendungsbereiche ohne eGK-Bezug ermöglicht.

Die Krankenkassen sind ab dem 15.01.2025 verpflichtet, jedem Versicherten, der nach vorheriger Information gemäß § 343 SGB V der Einrichtung einer ePA gegenüber der Krankenkasse nicht innerhalb einer Frist von sechs Wochen widersprochen hat (Opt-Out), eine nach § 325 Abs. 1 SGB V von der gematik zugelassene ePA zur Verfügung zu stellen. Daneben gibt es Anwendungen in der TI, die keinen direkten oder lediglich sekundären Kassenbezug aufweisen. Die gematik ist für die Zulassung dieser Anwendungen (z.B. Notfalldatenmanagement, e-Rezept, elektronischen Medikationsplan, Kommunikation im Medizinwesen zur Übermittlung einer elektronischen AU) verantwortlich[83].

8.2 Digitale Verwaltungsleistungen

Durch das OZG vom 18.08.2017 wurde die gesamte öffentliche Verwaltung, also auch die SV-Träger, verpflichtet, bis zum Jahr 2022 sämtliche Verwaltungsleistungen zusätzlich auch digital anzubieten. Die abzubildenden Verwaltungs- bzw. Leistungsangebote sind als Bündel über sogenannte Verwaltungsportale zur Verfügung zu stellen.

Im Bereich der Krankenkassen handelt es sich hierbei um Kernprozesse wie z. B. die Beantragung von Leistungen, das Einreichen bzw. die Aktualisierung von Lichtbildern für die eGK oder die Mitwirkungspflichten der Versicherten im Rahmen der Beantwortung des Unfallfragebogens oder des Bestandspflegebogens bei der Familienversicherung.

[83] Weitere Informationen abrufbar unter: www.gematik.de

Der GKV-SV übernimmt im Rahmen des OZG für seine Mitgliedskassen die zentrale Anbindung der Fachportale und Onlinegeschäftsstellen an das Bundesportal und somit die Weiterleitung der Versicherten bzw. Bürgerinnen und Bürger zu den jeweiligen Mitgliedskassen. Die zu digitalisierenden Kassenleistungen werden im sog. GKV-60-Leistungskatalog dargestellt. Über dessen Umsetzung und den Stand der Digitalisierung bei den Krankenkassen berichtet der GKV-SV gemäß § 217 f Abs. 2a SGB V jährlich dem BMG.

8.3 Fanpages

Der EuGH stellte in seinem bedeutsamen Urteil in Sachen “Facebook-Fanpages“ (Urteil vom 05.06.2018 – C 210/16) fest, dass sowohl Facebook, als auch die Fanpage-Betreiber gemeinsam für die Datenverarbeitung verantwortlich sind.
Als gemeinsam mit Meta Platforms Verantwortliche müssen Fanpage-Betreiber die Vorgaben der DSGVO einhalten und dazu – unter anderem – eine Vereinbarung über die gemeinsame Verantwortung schließen, der die Anforderungen von Art. 26 DSGVO erfüllt. Das aktuelle von Meta Platforms vorgelegte Addendum erfüllt diese Anforderungen nicht. Wissen Verantwortliche nicht genau, welche Datenverarbeitung stattfindet, können sie eine rechtskonforme Verarbeitung der personenbezogenen Daten nicht sicherstellen. Das betrifft auch die Frage, in welchem Umfang eine Übermittlung personenbezogener in das außereuropäische Ausland stattfindet. Eine solche ist nämlich nur dann zulässig, wenn die Vorgaben der Art. 44 ff. DSGVO eingehalten werden.

Nach dem Urteil des Verwaltungsgerichtes Köln vom 17.07.2025[84] sind Fanpages auf den sozialen Netzwerken wie „Facebook“ insbesondere auch durch Behörden zulässig, um Informationen zu verbreiten oder öffentlich zu kommunizieren. Über diesen Sachverhalt ist noch nicht abschließend geurteilt worden.

8.4 Digitale Versorgung

8.4.1 Digitale Gesundheitsanwendungen (DiGA)

Mit dem Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgungsgesetz - DVG) ist eine eigene Rechtsgrundlage für den Einsatz und die Nutzung digitaler Gesundheitsanwendungen geschaffen worden. Siehe hierzu die Veröffentlichung des Digitalausschusses des BAS.[85] Bei Apps ist generell zu unterscheiden zwischen vom BfArM zugelassenen DiGA, die entweder nach ärztlicher Verordnung oder nach Genehmigung durch die Krankenkasse zur Verfügung gestellt werden, und sonstigen Apps, die von den SV-Trägern angeboten werden (s. Punkt 4.3.4).

Die Digitale-Gesundheitsanwendungen-Verordnung (DiGAV), welche zum 21. April 2020 in Kraft getreten ist, regelt u.a. das Nähere zum Verfahren und die Anforderungen an die Prüfung der Erstattungsfähigkeit von DiGA in der gesetzlichen Krankenversicherung. Insbesondere trifft die DiGAV auch Regelungen zu Anforderungen an Sicherheit, Funktionstauglichkeit, Datenschutz und Datensicherheit, an die Qualität von DiGA sowie an den Nachweis positiver Versorgungseffekte.

DiGA als Satzungsleistung

84 Verwaltungsgericht Köln vom 17.07.2025, Az. 13 K 1419/23; Bundesregierung darf ihre Facebook-Fanpage behalten - beck-online.pdf
85 Abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/fitness-und-gesundheits-apps-digitale-gesundheitsanwendungen/digitale-gesundheitsanwendungen/

Mit dem Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG) vom 14. Oktober 2020 wurde § 11 Abs. 6 SGB V dahingehend ergänzt, dass Krankenkassen in ihrer Satzung nun auch DiGA als zusätzliche, vom Gemeinsamen Bundesausschuss nicht ausgeschlossene, Leistungen in der fachlich gebotenen Qualität vorsehen können. Dies kann Impulse für den Einsatz digitaler Gesundheitsanwendungen unter Beteiligung weiterer Leistungserbringergruppen schaffen (BT-Drs. 19/20708). Durch die Aufnahme dieses Versorgungsbereichs in die Regelung des § 11 Abs. 6 SGB V wird den Krankenkassen ermöglicht, im Rahmen der durch § 33a SGB V vorgegebenen Grenzen ergänzende Satzungsleistungen vorzusehen.

8.4.2 Digitale Pflegeanwendungen (DiPA)

Ebenfalls neu eingeführt wurde mit dem Digitale-Versorgungs-und-Pflege-Modernisierungsgesetz (PDVPMG) ein Anspruch von Versicherten der Pflegeversicherung auf Nutzung von digitalen Pflegeanwendungen (DiPA) im ambulanten Bereich. DiPA zielen darauf ab, die Selbständigkeit und die Fähigkeiten der Pflegebedürftigen zu verbessern und einer Verschlimmerung der Pflegebedürftigkeit entgegenzuwirken. Sowohl bei DiGA als auch bei DiPA ist generell nach Apps zu unterscheiden, die vom BfArM zugelassenen sind, die nach ärztlicher Verordnung oder nach Genehmigung durch die Krankenkasse / Pflegekasse zur Verfügung gestellt werden, und sonstigen Apps, die von den SV-Trägern angeboten werden. Zwischen DiGA und DiPA besteht ein Subsidiaritätsverhältnis. Der Anspruch auf DiPA besteht nur, soweit die Anwendung nicht wegen Krankheit oder Behinderung von einem anderen zuständigen Leistungsträger zu leisten ist.

8.4.3 Digitale Identität / Gesundheits-ID

Digitale Identitäten im Gesundheitswesen sollen gem. § 291 Abs. 8 SGB V ab dem 01.01.2024 als Alternative zu eGK eingesetzt werden. Ab 2026 kommt eine weitere Funktion hinzu: Patientinnen und Patienten brauchen dann keine eGK mehr als Versicherungsnachweis in der Praxis, sondern können sich mit ihrer digitalen Identität ausweisen.[86]

8.5 Digitale Dienste

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ersetzt ab dem 14.05.2024 das TTDSG und ist das Gesetz zum Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten. Das Telemediengesetz (TMG) ist damit außer Kraft getreten. Betroffen sind alle Anbieter von Telemedien, also aller elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind.

8.5.1 Speicherung von Informationen auf Endgeräten

Nach § 25 Abs. 1 TDDDG ist die Speicherung von Informationen in der Endeinrichtung des Endnutzers nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Für Cookies und andere Tracking-Maßnahmen (sogenannte Browser-Fingerprinting (Erstellung eines individuellen digitalen Fingerabdrucks), die Nachverfolgung über Werbe-IDs, MAC-Adressen und IMEI-Nummern sowie Smarthome-An-

[86] Abrufbar unter: https://www.gematik.de/anwendungen/gesundheitsid

wendungen) ist weiterhin eine DSGVO-konforme Einwilligung der Nutzer erforderlich. Ausnahmen von diesem Grundsatz sind in § 25 Abs. 2 TDDDG für technisch zwingend notwendige Zugriffe geregelt. Aus Art. 7 Abs. 3 DSGVO geht hervor, dass der Widerruf der Einwilligung genau so simpel möglich sein muss wie die Erteilung der Einwilligung.

8.5.2 Einwilligungsverordnung

Die auf § 26 Abs. 1 TDDDG basierende Einwilligungsverordnung (EinwVO) konkretisiert die Anforderungen an die Einwilligung zur Speicherung und zum Auslesen von Informationen auf Endeinrichtungen, etwa durch Cookies oder ähnliche Technologien. Sie stellt sicher, dass die Einwilligung freiwillig, spezifisch, informiert und eindeutig erfolgt. Dabei muss die Einwilligung aktiv erteilt werden – etwa durch eine bewusste Handlung, wie das Anklicken einer Schaltfläche. Die Verordnung verpflichtet Anbieter dazu, umfassend über Zweck, Umfang und Empfänger der Datenverarbeitung zu informieren.

Ein zentrales Element der EinwVO ist die Einführung sogenannter Einwilligungsverwaltungsdienste (Consent Management Provider), die Einwilligungen nutzerfreundlich und standardisiert verwalten. Diese Dienste sollen es Nutzerinnen und Nutzern ermöglichen, ihre Einwilligungen zentral zu erteilen, zu verwalten und zu widerrufen. Zudem legt die Verordnung technische und organisatorische Anforderungen an solche Dienste fest, etwa zur Sicherheit, Transparenz und Interoperabilität.

8.5.3 Eingebundene Videos

Auf den Webseiten der SV-Träger werden zur Erfüllung ihrer Informationspflicht nach § 3 EGovG auch Videos eingesetzt, dies können sowohl eigene als auch von Dritten eingebundene Videos sein. Beim Öffnen eines Videos werden Informationen als Cookies lokal gespeichert, welche der Analyse des Nutzerverhaltens und der Statistik dienen. Diese sind als nicht technisch notwendig anzusehen. Von daher wird die Einbettung von Videos aus datenschutzrechtlicher Sicht nicht ohne eine wirksame Einwilligung möglich sein.[87]

[87] Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2023/Rundschreiben-Telemedien-02-2023.html
siehe dazu auch: https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2025/13-teilautomatisierte-Webseitenpr%C3%BCfung.html

9 Künstliche Intelligenz (KI)

Anwendungen der Künstlichen Intelligenz (KI) werden bereits in verschiedenen Arbeitsbereichen der Sozialversicherungsträger eingesetzt. Die Verfahren können z. B im Rahmen der Sachbearbeitung oder Analysen von Verhalten bzw. Daten eigebunden werden. Sie können dabei als Bestandteile in teil- oder ggf. als vollautomatisierte Verfahren eigesetzt werden. Hierfür müssen die jeweiligen Voraussetzungen gegeben sein.

9.1 Begriffsbestimmungen

Unter Künstlicher Intelligenz versteht man Systeme, die in der Lage sind, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. Dies umfasst das Erkennen von Mustern, das Lernen aus Erfahrungen und das Treffen von Entscheidungen. Ein KI-System nutzt verschiedene Bestandteile, um seine Aufgaben ausführen zu können:

Maschinelles Lernen (ML):
Hierbei lernt ein Algorithmus eigenständig aus Daten, anstatt starr programmiert zu werden. Ein Lernalgorithmus bildet vorgegebene Beispieldaten auf ein mathematisches Modell ab. Dabei passt der Lernalgorithmus das Modell so an, dass es von den Beispieldaten auf neue Fälle verallgemeinern kann. Dieser Vorgang wird Training genannt. Nach dem Training ist der gefundene Lösungsweg im Modell gespeichert. Er wird nicht explizit programmiert. Das trainierte Modell kann für neue Daten Vorhersagen treffen oder Empfehlungen und Entscheidungen erzeugen.

Künstliche Neuronale Netze (KNN):
Diese sind dem menschlichen Gehirn nachempfunden. Sie bestehen aus Schichten von Neuronen (mathematischen Funktionen), die Informationen verarbeiten und gewichten. KNN werden beim maschinellen Lernen eingesetzt. Damit können Computer Probleme lösen, die zu kompliziert sind, um sie mit Regeln zu beschreiben, zu denen es aber viele Daten gibt, die als Beispiele für die gewünschte Lösung dienen können. KNN bilden die Basis für Deep Learning, das erhebliche Fortschritte bei der Analyse von großen Datenmengen erlaubt hat. Erfolgreiche Anwendungen des Deep Learning sind z. B. Bilderkennung und Spracherkennung.

Schwache und Starke KI:
Aktuelle Systeme sind „schwache KIs“, da sie nur in einem begrenzten Bereich (z. B. Schach, Wettervorhersage oder Textgenerierung) überzeugen. Um einen größeren Funktionsumfang zu erzielen, werden verschiedene KIs kombiniert, ein übergeordneter Agent wählt die zur Aufgabe passende KI automatisch aus. Eine „starke KI“, die über ein eigenes Bewusstsein und universelle Intelligenz verfügt, existiert bisher nur in der Theorie.

Eine KI ist kein einheitliches Gebilde, sondern nutzt je nach Anwendungsfall spezialisierte Modelle:

Transformer-Modelle:
Sie bilden das Rückgrat moderner mathematischer Sprachmodelle (Large Language Modell, LLMs). Durch das Training mit riesigen Datenmengen können sie die Beziehung zwischen Wörtern in langen Sätzen verstehen und Kontext präzise erfassen.

Convolutional Neural Networks (CNNs):
Diese Modelle sind auf die Verarbeitung von Bilddaten spezialisiert. Sie extrahieren Merkmale wie Kanten, Formen und Objekte und werden in der Gesichtserkennung sowie der medizinischen Bildanalyse eingesetzt.

Generative Adversarial Networks (GANs):
Hierbei werden zwei Netzwerke, gegeneinander trainiert. Eines versucht Daten zu generieren, die einem ursprünglichen Datensatz sehr ähnlich sind, das andere versucht echte und falsche Daten zu unterscheiden. Nach dem Training kann ersteres genutzt werden, um Daten zu generieren, die den ursprünglichen Daten sehr ähnlich sind. Dies führt z.B. zu extrem realistischen Ergebnissen bei der Erzeugung von synthetischen Bildern oder Stimmen.
Der Übergang von klassischer Software zu KI ist ein fundamentaler Wechsel in der Informatik. In der bisherigen, regelbasierten Software schreibt der Mensch jede Regel explizit vor (z. B. „Wenn Betrag > 1000, dann Prüfung erforderlich“). Das System ist transparent und logisch nachvollziehbar, aber starr. Nicht nur die Regeln, auch der Zustand der vorliegenden Daten muss genau definiert sein.

KI-Systeme arbeiten mit Wahrscheinlichkeiten. Sie erkennen Muster in Daten, die für Menschen oft zu komplex sind. Während sie flexibler sind als regelbasierte Software, bleibt die genaue Entscheidungsfindung der KI oft eine „Black Box“, da Millionen von Parametern gleichzeitig wirken.

Der Einsatz von KI im Zusammenhang mit personenbezogenen Daten birgt rechtliche und gesellschaftliche Risiken, z.B.:

Deanonymisierung: KI kann aus scheinbar anonymen Datensätzen durch Querverweise die Identität von Personen wiederherstellen.

Voreingenommenheit (Bias): Da KIs aus historischen Daten lernen, reproduzieren sie oft menschliche Vorurteile. Dies kann zu Diskriminierung z.B. bei Bewerbungsprozessen oder der Kreditvergabe führen.

Recht auf Vergessenwerden: In der DSGVO ist die Löschung von Daten verankert. Technisch ist es jedoch extrem schwierig, einmal „gelerntes“ Wissen über eine Person aus einem KI-Modell selektiv zu entfernen, ohne das gesamte Modell neu zu trainieren.

Profiling und Nudging (unbewusste Beeinflussung): Die Vorhersagekraft der KI erlaubt es, die psychologischen Schwachstellen von Menschen gezielt für Manipulation (z. B. im Wahlkampf oder Marketing) zu nutzen.
Zusätzlich zu den ethischen Risiken gibt es rein technische Schwierigkeiten beim Schutz personenbezogener Daten während des Trainingsprozesses.

Inversion-Angriffe: Forscher haben gezeigt, dass es möglich ist, durch gezielte Abfragen eines fertigen KI-Modells Rückschlüsse auf die ursprünglichen Trainingsdaten zu ziehen. Wenn das Modell mit privaten Daten trainiert wurde, könnten diese so teilweise wiederhergestellt werden.

Das Overfitting-Problem: Wenn ein Modell zu stark auf einen Datensatz trainiert wird, lernt es Einzelfälle auswendig, anstatt allgemeine Regeln zu finden. In diesem Fall gibt die KI keine allgemeinen Antworten mehr, sondern gibt womöglich exakte, private Daten einer realen Person preis.

Gegenmaßnahmen:
Um diese Probleme zu lösen, werden Techniken wie Differential Privacy (Hinzufügen von Rauschen zur Unkenntlichmachung) oder Federated Learning (Dezentrales Training auf dem Endgerät des Nutzers) entwickelt. Diese Verfahren stehen jedoch oft im Konflikt mit der Effizienz und Genauigkeit der KI-Modelle.

9.2 Einsatz von KI

Die möglichen Einsatzgebiete der KI sind ganzheitlich in Bezug auf Risiken und Chancen zu bewerten, insbesondere, wenn personenbezogene Daten verarbeitet werden. Hierzu verweisen wir im besonderen Maße auf die Ausführungen des Abschnitts 1 „Planung, Vorgehen, Gestaltung der Verfahren“ sowie Abschnitt 2 „Datenschutz“ dieses Leitfadens.
Gemäß § 67 c Abs. 3 SGB X dürfen die in § 35 SGB I genannten Stellen Sozialdaten, die von Ihnen für andere Zwecke erhoben wurden, unter weiteren Voraussetzungen auch zum Entwickeln von KI-Modellen und KI-Systemen speichern, verändern oder nutzen. Voraussetzungen hierfür sind unter anderem:

- die KI-Systeme dienen der Erfüllung einer gesetzlichen Aufgabe nach dem SGB,
- die Daten sind erforderlich,
- die Verwendung von anonymisierten Daten führt zu einer Verfälschung der Verarbeitungsergebnisse und Sozialdaten werden pseudonymisiert.

Die Europäische Union hat im Dezember 2023 eine Einigung über eine KI-Verordnung (AI Act) erzielt. Der Gesetzestext wurde am 13. März 2024 verabschiedet. Die KI-Verordnung legt unter anderem harmonisierte Vorschriften für den Betrieb fest, verbietet bestimmte Praktiken und stellt besondere Anforderungen an Hochrisiko-KI-Systeme und schließt in Art. 2 auch explizit Betreiber von KI-Systemen in den Anwendungsbereich ein.
Um KI-Systeme verantwortungsvoll zu nutzen, ist ein tragfähiges Managementsystems für Künstliche Intelligenz (AIMS) unerlässlich. Als internationaler Standard zur Implementierung gilt die Norm ISO / IEC 42001:2023 „Information technology- Artificial Intelligence-Management System“. Die Norm ist gemäß dem B3S-GKV-PV bei der Benutzung und der Entwicklung von KI-Systemen zu berücksichtigen. Sie verfolgt ein ganzheitliches Vorgehen: Ausgehend von der Analyse der eigenen Institution erfolgt unter anderem die Erstellung einer Policy sowie die Zuweisung von Rollen und Verantwortlichkeiten. Darüber hinaus werden alle Phasen des KI-Lebenszyklus, von der Planung über Entwicklung und Betrieb bis zur kontinuierlichen Verbesserung betrachtet. Die Norm umfasst neben diesem normativen Teil insgesamt vier Anhänge, die unter anderem die ISO-Norm-typischen Controls, Umsetzungshilfen für diese Controls sowie KI-spezifische Risikoquellen vorgibt.

Sowohl der AI Act als auch die ISO / IEC sind an den Werten von Transparenz, Risikomanagement, klaren Verantwortlichkeiten und Sicherheit ausgerichtet. Auf der Grundlage dieses Regelwerks können beim Betrieb von KI-Systemen Risiken minimiert und damit ein verordnungskonformer Betrieb ermöglicht werden. Angesichts der vielfältigen Anwendungsszenarien und raschen Entwicklung von KI empfiehlt es sich darüber hinaus, die Handreichungen und Veröffentlichungen der relevanten Institutionen wie z. B. der Datenschutzbeauftragten des Bundes und der Länder zu prüfen.

9.3 Fachliche Anforderungen an den Einsatz von KI

Je nach Einsatzgebiet einer KI-Anwendung ist eine Klassifizierung von KI-Systemen als Hochrisiko-Systeme vorzunehmen, die besonderen Anforderungen genügen müssen. Die Einstufungskriterien ergeben sich aus Art. 6 der KI-Verordnung in Verbindung mit Anhang II. Auch wenn nicht alle möglichen Einsatzgebiete bei den SV-Trägern dieser strengeren Klassifizierung nachkommen werden, gehen wir nachfolgend hiervon aus, da bei Daten aus Gesundheitsthemen ein Hochrisiko-System vorliegt.

Die einzuhaltenden Prüfverfahren (Konformitätsbewertungsverfahren) müssen bereits im Vorfeld des Einsatzes einer KI-Anwendung durchgeführt werden und ergeben sich aus Art. 16 Buchst. F i. V. m. Art. 43 Abs. 1 und 2 der KI-Verordnung. Das hier einzuhaltende interne Konformitätsverfahren ist nach Anhang VI der Verordnung vom Anbieter selbst auf der

Grundlage einer internen Kontrolle der Einhaltung der materiellen Anforderungen durchzuführen. Basis der Bewertung ist die technische Dokumentation (Art. 11 KI-Verordnung i. V. m. Anhang VI Nr. 2).
Für Hochrisiko-KI-Systeme ist zudem ein kontinuierlicher Risikomanagementsystem-Prozess einzurichten. Für Behörden wie Träger gilt nach Art. 27 KI-Verordnung auch, dass eine Grundrechte-Folgenabschätzung vorgenommen werden muss.
Werden Techniken eingesetzt, bei denen Modelle mit Daten trainiert werden, gelten geeignete Daten-Governance- und Datenverwaltungsverfahren. Es sind besondere Aufzeichnungspflichten zu beachten sowie Anforderungen an technische Dokumentationen, die vor der Verkehrseinführung zu erstellen und immer auf dem neuesten Stand zu halten sind (Art. 11, 12 KI-Verordnung).[88]

Nutzer von KI-Systemen sind über den Einsatz bzw. die Art der Erstellung in Kenntnis zu setzen, wenn Ergebnisse einer KI-Anwendung einer Person zukommen.

[88] Ausführlich Chibanguza/Steeg, NJW 2024, 1769 ff. und Gerdemann, NJW 2024, 2209 ff.