Die Prüfdienste des Bundes
und der Länder informieren

Leitfaden

Elektronische Kommunikation
und
Digitalisierung in der Sozialversicherung

Version 6.1.1
Stand: 19.04.2024

Version:	Datum:	Grund d. Änderung:	Bearbeiter:
4.0	Oktober 2014	Einarbeitung EGovG, Neustrukturierung gesamtes Dokument (aus Version 3.5).	AK Signatur
4.1	April 2016	Einarbeitung 5. SGB-IV-ÄndG, Anforderungen „Online-Geschäftsstelle“, Anforderungen Apps	AK E-Kommunikation
5.0	September 2018 / Mai 2019	Neustrukturierung und Aktualisierung	AK E-Kommunikation
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
6.1.1	April 2024	Überarbeitung des Leitfadens	AK E-Kommunikation und Digitalisierung in der Sozialversicherung

Herausgeber:

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

Tel.: (0211) 855-5
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)
  Tel.: (04471) 1807-0
- Referat 611
  Tel.: (0228) 619-2611

E-Mail:
LeitfadenElektronischeKommunikation@bas.bund.de

Wesentliche Änderungen zu Version 6.1

Neu aufgenommen

- Punkt 5.4 Maschinelles Lernen und Anwendungen der Künstlichen Intelligenz
- Punkt 6.9 Nutzung von Gesundheitsdaten
- Punkt 8.5 Telemedien

Änderungen / Ergänzungen

- Punkt 1.4.6 IT-Sicherheit / Datensicherheit
  - Inhaltliche Überarbeitung
- Punkt 1.6 Einrichtung und Betrieb eines Hinweisgebersystems
  - Inhaltliche Überarbeitung
- Punkt 4.1.2 Schriftformerfordernis und Ersatz der Schriftform
  - Anpassung in Bezug auf §§ 36a SGB I, 13 EGovG
- Punkt 4.2.1 Grundsätze zum Zugang / Eröffnung der Kommunikation
  - Anpassung in Bezug auf § 36 a SGB I
- Punkt 4.2.2 Zugangsmöglichkeiten bei Schriftformersatz
  - Anpassungen in Bezug auf § 36 a SGB I
- Punkt 4.2.2.5 Der elektronische Widerspruch bei den SV-Trägern
  - Anpassung in Bezug auf § 36 a SGB I
- Punkt 5.2.1 Materielles Fachrecht
  - Inhaltliche Überarbeitung
- Punkt 7.2.2 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen
  - Inhaltliche Überarbeitung
- Punkt 7.5 Datenspeicherung in der Cloud
  - Inhaltliche Überarbeitung
- Punkt 8.1 Telematikinfrastruktur (TI)
  - Inhaltliche Überarbeitung
- Punkt 8.4 Digitale Versorgung – Digitale Gesundheitsanwendungen (DiGA)
  - Inhaltliche Überarbeitung

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 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

Der Abschnitt „Planung / Vorgehen / Gestaltung der Verfahren“ 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 lediglich um die Überarbeitung eines abgegrenzten, digitalen Informationsangebotes, die Entwicklung bzw. Erweiterung einer Online-Geschäftsstelle oder gar 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. Alle nachfolgend genannten Schritte tragen aus Sicht der Prüfdienste des Bundes und der Länder zum Projekterfolg und der Reduzierung von Risiken bei.

Bei den Schritten handelt es sich um:

- Erstellung eines Projektvorschlages / Projektanbahnung

- Vorbereitende Analysen und Maßnahmen
  - Geschäftsprozessanalyse und -optimierung
  - Datenschutzrechtliche Anforderungen an Gestaltung von Verfahren
  - Berücksichtigung von Art. 25 DSGVO (Datenschutz durch Technik)
  - Berücksichtigung von Art. 32 DSGVO (Sicherheit der Verarbeitung)
  - Datenschutz-Folgenabschätzung
  - Einrichtung eines Meldewesens bei Datenschutzverletzungen

- Begleitende und nachgehende Betrachtung
  - Zielerreichung
  - Wirtschaftlichkeitsbetrachtung
  - Bewertung Risikomanagement / Compliance
  - Anzeigen an Aufsichtsbehörden
  - IT-Sicherheit / Datensicherheit
  - Risikomanagement / Compliance / Interne Kontrollsysteme
  - Change Management

Eine Geschäftsprozessanalyse und ggf. -optimierung, Analysen und Festlegungen zu Datenschutz und Datensicherheit, Wirtschaftlichkeitsbetrachtungen sowie – falls keine ausdrücklichen Ausnahmetatbestände vorliegen – die Anzeige 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 oder der Rational Unified Process; 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.

Um die Lesbarkeit dieses Dokuments zu verbessern, werden wir uns bei Schutzbedarf auf die Kategorien des BSI-Standard 200_2 „normal“, „hoch“ und „sehr hoch“ beziehen, ohne explizit auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit einzugehen. Dabei beziehen wir uns jeweils auf das höchste Schutzniveau der genannten Schutzziele.

Für das Vertrauensniveau verwenden wir die Kategorien des Standards der eIDAS-Verordnung „niedrig“, „substantiell“ und „hoch“.

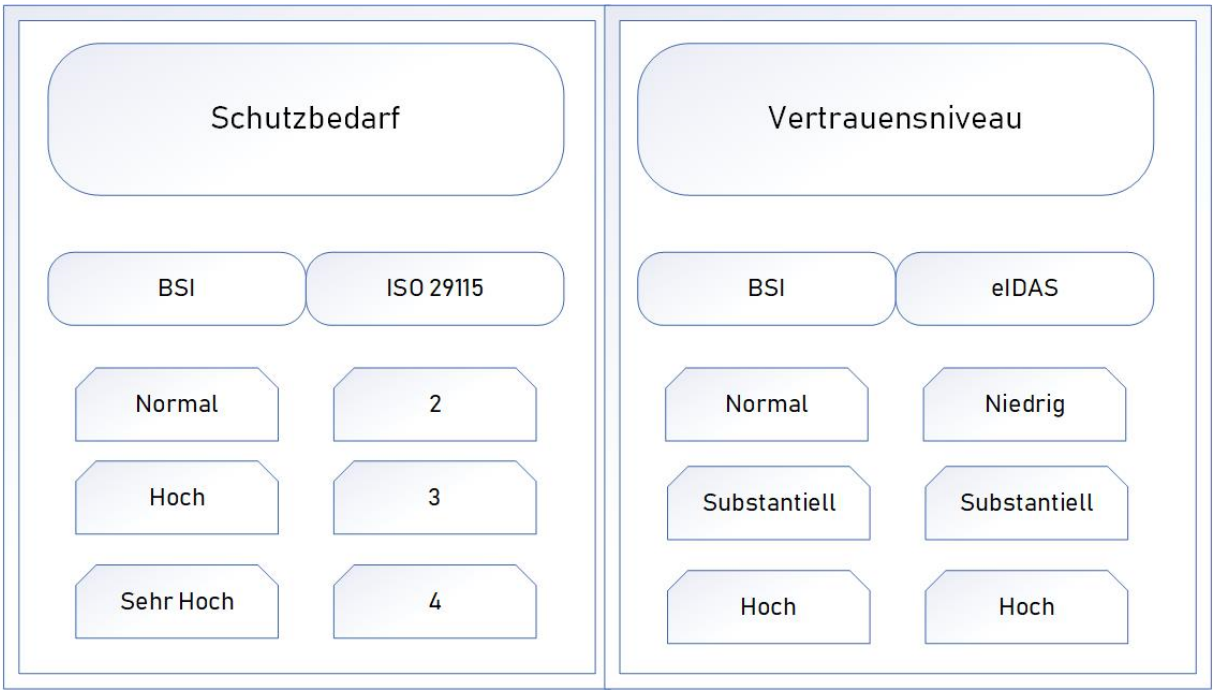

Abbildung 1 Schutzbedarf, Vertrauensniveau

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 **Betrachtung der Ausgangslage** können ggf. vorhandene Schwächen ermittelt und bewertet werden. Sollten keine erheblichen Schwachstellen zu finden sein und auch keine rechtlichen Vorgaben eine Änderung erforderlich machen, so ist bereits an dieser Stelle zu hinterfragen, ob das Projekt überhaupt durchgeführt werden muss.

Wurden Schwächen identifiziert, so stellt deren Behebung den Ausgangspunkt für die Formulierung konkreter **Projektziele** dar. Weitere Ansätze für die Projektziele können die Gesamtstrategie der Organisation oder deren IT-Strategie sowie die Erfüllung neuer rechtlicher Vorgaben liefern. Grundsätzlich gilt, dass nicht das neue Verfahren die Ziele definieren sollte, sondern umgekehrt – anders ausgedrückt: es sollte nicht erst das Softwareprodukt ausgesucht werden und dann die Einsatzmöglichkeit.

Die Projektziele sollten so festgelegt und formuliert sein, dass deren Erreichung später überprüft werden kann. Auch die Buchung der Kosten eines Projekts ist abhängig von dessen Zielen. Liegt die Zielsetzung eines Projektes im Bereich gesundheitliche Aufklärung oder auch Mitgliederwerbung, so sind die Kosten auch dann auf den entsprechenden Konten zu verbuchen, wenn für die Umsetzung des Projektes informationstechnische Lösungen verwendet werden.

Unabhängig davon, ob die Projektziele aus der Gesamt- oder der IT-Strategie hergeleitet wurden, sich aus Schwächen der bisherigen Prozesse oder aus rechtlichen Anforderungen 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 bzgl. der organisatorischen und technischen Umsetzung des einzuführenden oder zu ändernden Verfahrens. Auch wenn die Ausgestaltung in dieser Phase i.d.R. noch nicht endgültig bekannt sein dürfte, sollte eine **allgemeine Verfahrensbeschreibung** erstellt werden. Davon ausgehend kann eine erste Abschätzung der zu erwartenden **Risiken** sowie der **Wirtschaftlichkeit** vorgenommen werden. Eine detaillierte Risikoanalyse sowie Wirtschaftlichkeitsbetrachtungen sind erst in den folgenden Projektphasen vorzunehmen.

Schon in dieser frühen Phase sollte auch geprüft werden, ob **Wechselwirkungen** mit anderen Verfahren oder Geschäftsprozessen bestehen oder möglich sind. Andere betroffene Fachbereiche des SV-Trägers können so rechtzeitig informiert und beteiligt werden. Auf diese Weise können gegenläufige Entwicklungen vermieden und möglicherweise Synergieeffekte genutzt werden. 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 ist von den entsprechenden Stellen zu entscheiden, ob das Projekt begonnen werden soll; ob eine ggf. vorgestellte Lösung umgesetzt wird, kann zu diesem Zeitpunkt noch nicht entschieden werden, da hierfür im Projekt erst die Entscheidungsgrundlagen erarbeitet werden müssen.

Wurde beschlossen, dass ein Projekt begonnen werden soll, so müssen anfangs zahlreiche allgemeine Aufgaben des Projektmanagements durchgeführt werden. Beispielsweise sollte ein Lenkungsausschuss gebildet, eine Projektleitung ernannt, ein Projektplan erstellt sowie die erforderlichen personellen, materiellen und finanziellen Ressourcen angemeldet und gesichert werden.

1.3 Vorbereitende Analysen und Maßnahmen

1.3.1 Geschäftsprozessanalyse und -optimierung

In den allermeisten Fällen stehen elektronische Verfahren nicht für sich, sondern dienen vornehmlich dem Ziel, **Geschäftsprozesse zu unterstützen**. 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 (auch mit fachlichen 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 oder Automatisierung). 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 den fachlichen und technischen Anforderungen und 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 nicht die an sie gestellten Erwartungen erfüllen oder die Prozesse nicht korrekt umgesetzt werden. Aus diesem Grund sollten die Prozesse nach einer gewissen 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 insbesondere durch die DSGVO neue Anforderungen entstanden. Diese sind bereits frühzeitig in der Planung und Entwicklung zu berücksichtigen[4].

---

[2] Zum eigenen Feld der strategischen Ansätze beim Einsatz von IT (insbes. IT-Strategie, IT-Organisation) siehe die „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik“, Stand August 2020, abrufbar unter:
https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/ver%C3%B6ffentlichungen_brh_lrh/it-mindestanforderungen.pdf?__blob=publicationFile&v=4

[3] https://www.verwaltung-innovativ.de/DE/Organisation/Organisationshandbuch/organisationshandbuch_node.html

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder „Standard Datenschutzmodell: Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele“ (Version 2.0b), abrufbar unter:
https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html

Dabei handelt es sich nicht allein um technische Anforderungen, die bei der Programmierung etc. zu beachten sind, sondern auch um Fragen der Verfahrensgestaltung. Daher sind auch bei der Entwicklung frühzeitig die Bereiche IT, übergreifende Bereiche (Organisation, Datenschutz etc.) sowie die Fachbereiche einzubeziehen.

Die entsprechenden Abwägungen zur Wahl der Maßnahmen und Ausgestaltung der Verfahren sollten frühzeitig erfolgen und auch nachvollziehbar dokumentiert werden.

1.3.2.1 Art. 25 DSGVO

Art. 25 DSGVO verpflichtet die Verantwortlichen in seinen Absätzen 1 und 2 zu folgenden Punkten:

- Datenschutz durch Technik – „data protection by design“
  Die Verantwortlichen werden dabei verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen.
  Im Rahmen der Erörterung von entsprechenden Maßnahmen (z. B. Pseudonymisierung) sollte eine vorgenommene Abwägung und objektive Bewertung von Umständen, wie dem Stand der Technik, Implementierungskosten und auch Risiken für Rechte und Freiheiten der Betroffenen, dokumentiert werden.
- Datenschutz durch Voreinstellung – „data protection by Default“
  Die Verantwortlichen werden verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellungen im technischen Verfahren grundsätzlich nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind.[5]
  Dabei gilt die Verpflichtung, die Voreinstellungen entsprechend für die Frage der Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit auszurichten.[6]
  Im Rahmen der Erörterung von entsprechenden Maßnahmen sollten auch an dieser Stelle vorgenommene Diskussionen und Abwägungen dokumentiert werden.

1.3.2.2 Art. 32 DSGVO

Art. 32 DSGVO regelt – als Querschnittsthema - die Sicherheit der Verarbeitung personenbezogener Daten und damit, wer welche technischen und organisatorischen Maßnahmen treffen muss, um ein angemessenes Schutzniveau bei der Verarbeitung sicherzustellen.
Dabei ist zur Bestimmung der geeigneten und angemessenen Maßnahmen abzuwägen (Verhältnismäßigkeit):

- Stand der Technik (das technisch Mögliche und Erprobte; hier ist das europarechtliche Begriffsverständnis zu Grunde zu legen)
- Kosten
- Art und Weise der Verarbeitung
- mögliche Schäden (Risiken für Rechte und Freiheiten der natürlichen Personen)[7]

Auch diese Erörterungen sind zu dokumentieren.

---

[5] BeckOK DatenSR/Paulus DSGVO Art. 25 Rn. 8.
[6] BeckOK DatenSR/Paulus DSGVO Art. 25 Rn.10.
[7] Jandt in Kühling / Buchner DSGVO, Art. 32, ab Rn. 7.

Die Umsetzung der Erörterungen bzw. technisch-organisatorischen Maßnahmen im Prozess sollten im weiteren Verlauf der Umsetzung festgehalten werden.

1.3.3 Datenschutz-Folgenabschätzung

Die entsprechenden Maßnahmen der vorgenannten datenschutzrechtlichen Betrachtungen sind dann im Rahmen einer ggf. erforderlichen Datenschutz-Folgenabschätzung einzubringen (siehe Abschnitt Datenschutz Pkt. 2.7)[8].

Eine Datenschutz-Folgenabschätzung ist vor Einführung eines Verarbeitungsvorgangs durchzuführen und im Falle von Verfahrensänderungen gegebenenfalls anzupassen.

1.3.4 Einrichtung eines Meldewesens bei Datenschutzverletzungen

Neben den Anforderungen an die Gestaltung von Verfahren sind ggf. auch neue Verfahren an sich zu errichten.

Dabei ist die frühzeitige Ausgestaltung eines trägerinternen und externen Meldeverfahrens bei künftigen Verletzungen des Schutzes personenbezogener Daten bereits im Rahmen der Umsetzungsphase von Vorhaben zu berücksichtigen. Die entsprechenden Bereiche des SV-Trägers (insbesondere Datenschutzbeauftragte) sind vorzugsweise bereits in der Konzeptionsphase einzubinden.

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.

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.

[8] Siehe z. B. Art. 29-Gruppe, Working Paper 249, Punkt 9.

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, 6 Satz 2 EGovG). Hierfür

sind die gängigen Verfahren zur Wirtschaftlichkeitsberechnung[9] (§ 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 / Compliance

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

Maßnahmen zu deren Bewältigung sind zu entwickeln und auch noch im Wirkbetrieb fortzuschreiben.

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 internen Richtlinien) zu setzen, deren Einhaltung durch das Compliance-System der Träger

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

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 sicherzustellen. 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.[10]

1.4.4 Vergabeverfahren

Nach § 22 SVHV muss dem Abschluss von Verträgen über Lieferungen und Leistungen mit Ausnahme der Verträge, die der Erbringung gesetzlicher oder satzungsmäßiger Versicherungsleistungen dienen, eine öffentliche Ausschreibung vorausgehen. Hiervon kann in Ausnahmefällen abgesehen werden, sofern die Natur des Geschäfts oder besondere Umstände dies rechtfertigen. Landesspezifische Regelungen sind ggf. zu beachten.

Hinweis:
Der Beauftragte der Bundesregierung für Informationstechnik (www.cio.bund.de) hat für die Beschaffung von IT-Leistungen für die Bundesverwaltung ergänzende Vertragsbestimmungen (EVB-IT) für den Abschluss von Verträgen mit externen Anbietern erarbeitet. Die Verträge sollen den öffentlichen Auftraggeber davor schützen, durch die allgemeinen Vertragsbedingungen des Anbieters benachteiligt zu werden.

Die Prüfdienste des Bundes und der Länder raten dringend, die Empfehlungen zu beachten. Näheres über die jeweiligen Vertragswerke sind der o.g. Internetseite zu entnehmen.

1.4.5 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 SGV 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.

[10] Zum Aufbau eines Compliance Managements siehe Bundesamt für Sicherheit in der Informationstechnik ORP.5: Compliance Management (Anforderungsmanagement) (Edition 2021), abrufbar unter
Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_5_Compliance_Management_Editon_2021.html

Die Aufsichtsbehörden haben den „Grundleitfaden 85“[11] 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 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.[12]

1.4.6 IT-Sicherheit / Datensicherheit

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

Die BSI-KRITIS-Verordnung bestimmt (nach Anpassung mit Inkrafttreten am 30. Juni 2017 – Korb 2[13]) den Anwendungsbereich in der gesetzlichen Sozialversicherung. Diese hiervon betroffenen SV-Träger müssen nach § 8a BSI-Gesetz innerhalb von zwei Jahren die wesentlichen IT-Systeme entsprechend dem Stand der Technik absichern, hierüber regelmäßig geeignete Nachweise erbringen, eine Kontaktstelle benennen und erhebliche IT-Störungen unverzüglich dem BSI melden.

Betreiber Kritischer Infrastrukturen sind nach § 8a Abs. 3 BSIG gesetzlich verpflichtet, alle zwei 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 Informations-sicherheit (ISMS) und Geschäftskontinuität (Business Continuity Management System, BCMS) beim geprüften Betreiber.[14]

Bei Auslagerung von IT-Dienstleistungen verbleibt die Sicherheitsverantwortung auch beim KRITIS-Betreiber.[15]. Betreiber Kritischer Infrastrukturen 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. Mit dem IT-Sicherheitsgesetz 2.0 wurde für KRITIS-Betreiber im Mai 2021 ausdrücklich der Einsatz von Systemen zur Angriffserkennung im BSIG vorgeschrieben (§ 8a Abs. 1a BSIG). Diese Systeme stellen eine effektive Maßnahme zur Erkennung von Cyberangriffen dar und unterstützen insbesondere die Schadensreduktion. Die Betreiber mussten die Einführung eines Systems zur Angriffserkennung erstmalig bis zum 1. Mai 2023 gegenüber dem BSI nachweisen.

---

[11] 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/

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

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

[14] Die Lage der IT-sicherheit in Deutschland 2023, Digital Sicher BSI, S. 62

[15] Die Lage der IT-sicherheit in Deutschland 2023, Digital Sicher BSI, S. 59.

§ 392 SGB V in der Fassung des Digital-Gesetzes (DigiG) greift diese allgemeinen Anforderungen, die Systeme der Krankenkassen entsprechend dem Stand der Technik (siehe Art. 32 DS-GVO) zu halten und angemessene organisatorische und technische Vorkehrungen zu treffen für alle Träger der gesetzlichen Krankenversicherung verpflichtend auf und sieht zudem entsprechende vertragliche Verpflichtungen für deren Dienstleister vor. Grundlage hierfür bildet der Branchenspezifische Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer „B3S-GKV/PV“[16], an dessen Erstellung die Träger verpflichtend mitwirken sind mitzuwirken und dessen fachliche Eignung durch BSI festgestellt wird.

1.4.7 Risikomanagement / Compliance / Interne Kontrollsysteme

Die neuen bzw. geänderten Verfahren / Anwendungen sind durch die hierfür zuständigen Stellen der SV-Träger in das generelle Risikomanagement, die Compliance-Maßnahmen und das interne Kontrollsystem des SV-Trägers einzubeziehen.

Dabei sind insbesondere folgende Punkte vorzunehmen:

- Aufnahme in Verfahrensübersicht / Verarbeitungsverzeichnis
- Prüfung der Anwendungen / Systeme auf Einhaltung der allgemeinen Vorgaben des Risikomanagements / der Compliance
- Einbezug der Umsetzung / des Wirkbetriebs der Anwendungen / Systeme in Prüfplan der verantwortlichen Stellen.

1.4.8 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
- Datenschutz
- IT-Sicherheit
- Risikomanagement und Internes Kontrollsystem
- Speicherung und Archivierung

Eine nachvollziehbare Dokumentation des Änderungsprozesses ist dringend zu empfehlen.

[16] Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Textbausteine/DE/KRITIS/B3S/Finanz-Versicherungswesen/b3s-gkv-pv.html

1.5 Umsetzung der eIDAS-Verordnung

Die eIDAS-Verordnung[17] 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).[18]

Die Instrumente der Verordnung sind bei der Gestaltung der Authentifizierungs-/ Identifikationskonzepte der SV-Träger im Rahmen der elektronischen Kommunikation in die Überlegungen einzubeziehen (siehe § 36 a Abs. 2a Nr 3 lit. 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 jeden Mitarbeiter der juristischen Person erforderlich sind.

Elektronische Einschreibe- und Zustelldienste
Elektronische Einschreiben (§ 18 VDG) betreffen die Übermittlung von Daten mit elektronischen Mitteln. Erreicht werden kann dadurch der Nachweis für die Absendung durch identifizierte Absender sowie Zustellung / Empfang der Daten / Nachricht bei identifizierten Empfängern zu einem nachvollziehbaren Zeitpunkt. Auch die Rechtswirkung der Unversehrtheit der Daten, also der Schutz vor Verlust oder unbefugter Änderung (Integrität), ist gegeben.

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 QES ohne Smartcard / Lesegeräte.
Dadurch kann eine Authentifizierung auf hohem Niveau und gleichzeitig eine Nutzbarkeit für mobile Dienste erreicht werden.
Das Signaturverfahren verläuft dann – grob dargestellt – wie folgt:

- Grundlegende Authentifizierung des Anwenders für die Fernsignatur bei einem Vertrauensdienstanbieter (Identitätsfeststellung beim Vertrauensdienstanbieter durch Zwei-Faktor-Authentifizierung)
- Speicherung der Signaturschlüssel in sicheren Einheiten
- Vertrauensdienstanbieter versendet Code zum Auslösen der Fernsignatur an mobiles Gerät des Anwenders
- Auslösen der Fernsignatur beim Vertrauensdienstanbieter über Code am (mobilen oder anderen) Gerät
- Vertrauensdienstanbieter gibt nach Empfang des Codes des Anwenders das Signaturzertifikat für die Fernsignatur frei
- Als ggf. weitere (zweite) Faktoren können bei hohem Schutzbedarf dann weitere, auch auf mobilen Geräten einsetzbare Faktoren dienen (z. B. biometrische Funktionen)

[17] 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.
[18] Gesetz vom 18. Juli 2017, BGBl. 2017 I, S. 2745.

1.6 Einrichtung und Betrieb eines Hinweisgebersystems

Die Whistleblower Richtlinie (WBRL) mit der Umsetzung in nationales Gesetz verpflichtet Unternehmen mit durchschnittlich mehr als 50 Mitarbeitern (Unternehmen mit 50 - 249 Mitarbeitern hat der Gesetzgeber eine Übergangsfrist bis zum 17.12.2023 eingeräumt), einen Meldekanal zu implementieren und eine Meldestelle einzurichten.

Das Hinweisgeberschutzgesetz sieht die Verpflichtung zu einem Hinweisgebersystem vor. Dieses System muss wiederum entsprechend der in diesem Punkt 1. des Leitfadens erörterten allgemeinen Anforderungen an Verfahren des Trägers ausgestaltet sein. Dies betrift insbesondere die Punkte

- Durchführung einer Datenschutz-Folgeabschätzung
- Aufnahme in das Verfahrensverzeichnis und Datenschutzkonzept,
- Einrichtung der technisch-organisatorischen Maßnahmen (insbes. Ausgestaltung der Zugriffsrechte, Maßnahmen zu Geheimhaltung eingehender Informationen, Maßnahmen zum Schutz betroffener Personen und Mitarbeitender)
- Festlegung Speicherdauer und Löschfristen sowie -verfahren
- Einbezug in Verfahren zur Erfüllung der Rechte Betroffener (Informations- und Auskunftsverfahren).

Meldekanäle können intern von einer hierfür benannten Person oder Abteilung betrieben oder extern von einem Dritten bereitgestellt werden. Anhand einer Zuordnung an Strukturen der Institution könnte eine Angliederung z. B. an die HR-Abteilung, Rechtsabteilung, Compliance-Abteilung, Interne Revision oder Datenschutz (unter Beachtung möglicher Interessenskonflikte) erfolgen.

Zulässigkeit der Datenverarbeitung

Das Hinweisgeberschutzgesetz als nationale Umsetzungsnorm zu Art. 8 WBRL fungiert als Ermächtigungsgrundlage (Art. 6 Abs. 1 S. 1 lit.c DSGVO) für verpflichtete Unternehmen zur Verarbeitung von Daten (gem. Art. 4 Nr. 1 DSGVO). Unternehmen mit weniger als 50 Mitarbeitern werden nicht in den Anwendungsbereich des nationalen Rechts zur Umsetzung der WBRL fallen. Bei einer Interessenabwägung nach Art. 6 Abs. 1 S. 1lit. f DSGVO könnte der Abschluss einer Vereinbarung nach Art. 88 DSGVO i. V. m. § 26 Abs. 4 S. 1 BDSG empfehlenswert sein, dabei sind die Vorgaben der DSGVO für die Datenerhebung und –weiterverarbeitung zu berücksichtigen.

Das Datenschutzkonzept für den Meldekanal bzw. Meldeprozess sollte sich auf die Minimierung der datenschutzrechtlichen Risiken für die Rechte und Freiheiten der betroffenen Personen (Löschkonzept, Unterrichtungs- und Auskunftspflichten) fokussieren.

Eine Datenschutz-Folgenabschätzung ist vor Einführung eines Meldekanals zwingend durchzuführen. Verwiesen wird auf die Orientierungshilfe der Datenschutzkonferenz aus dem Jahr 2018.[19]

[19] Siehe Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

2 Datenschutz

2.1 Einleitung

Datenschutz ist Grundrechtsschutz und schützt das Recht des Bürgers auf informationelle Selbstbestimmung. Dies führt zwangsläufig zu einer Beschränkung der Befugnisse von dem Amtsermittlungsprinzip verpflichteten Sozialleistungsträgern.

Datenschutz wirkt präventiv. Wenn Daten an Unbefugte abfließen, ist der Schaden eingetreten. Für den erforderlichen Personenbezug gem. Art 4 Nr. 1 DSGVO genügt es, dass ein unmittelbarer Bezug zur Person des Betroffenen herstellbar ist. Letzteres ist bei anonymisierten Daten nicht der Fall. Weder die DSGVO noch BDSG und SGB X definieren, wann eine Anonymisierung erfolgt ist, und überlassen es der Rechtsanwendung, wann kein Personenbezug mehr besteht. Besondere Probleme bereitet in diesem Zusammenhang die schleichende Identifizierbarkeit aufgrund des technischen Fortschritts.

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 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.

Der Europäische Datenschutzausschuss (EDSA) gibt Hinweise in Form von Leitlinien zur einheitlichen Anwendung der Datenschutz-Grundverordnung (DSGVO)[20].

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 stets ein aktives Verhalten – nämlich eine „Willensbekundung“ - voraus, verlangt also die Opt-In-Lösung, Opt-Out scheidet damit zwangsläufig aus. Selbst konkludente Einwilligungen scheiden zumindest bei besonderen Kategorien von Daten aus, weil die Einwilligung dort „ausdrücklich“ zu erfolgen hat.
Die Freiwilligkeit der Einwilligung setzt jedenfalls die Einsichtsfähigkeit in die Tragweite der Entscheidung voraus.

Ein Konflikt mit Mitwirkungspflichten (§§ 60 ff SGB I) ist wegen Erwägungsgrund 43, wonach die Einwilligung keine gültige Rechtsgrundlage bei klarem Ungleichgewicht, „insbesondere, wenn es sich bei dem Verantwortlichen um eine Behörde handelt", abgeben sollte, zu befürchten. Erwägungsgründen kommt indes keine normative Funktion zu und die Einschränkung „…in Anbetracht aller Umstände…“ erlaubt eine restriktive Auslegung bei notwendigen Mitwirkungshandlungen. 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.

[20] Tätigkeitsbericht 2022 BfDI, S. 18 ff.

Die Prüfdienste empfehlen, ein Einwilligungsmanagement aufzusetzen, das sich auf alle technischen (z. B. Cookies) und fachlichen Anwendungsfälle (z. B. Kontaktaufnahme) bezieht (siehe auch Pkt. 8.5).

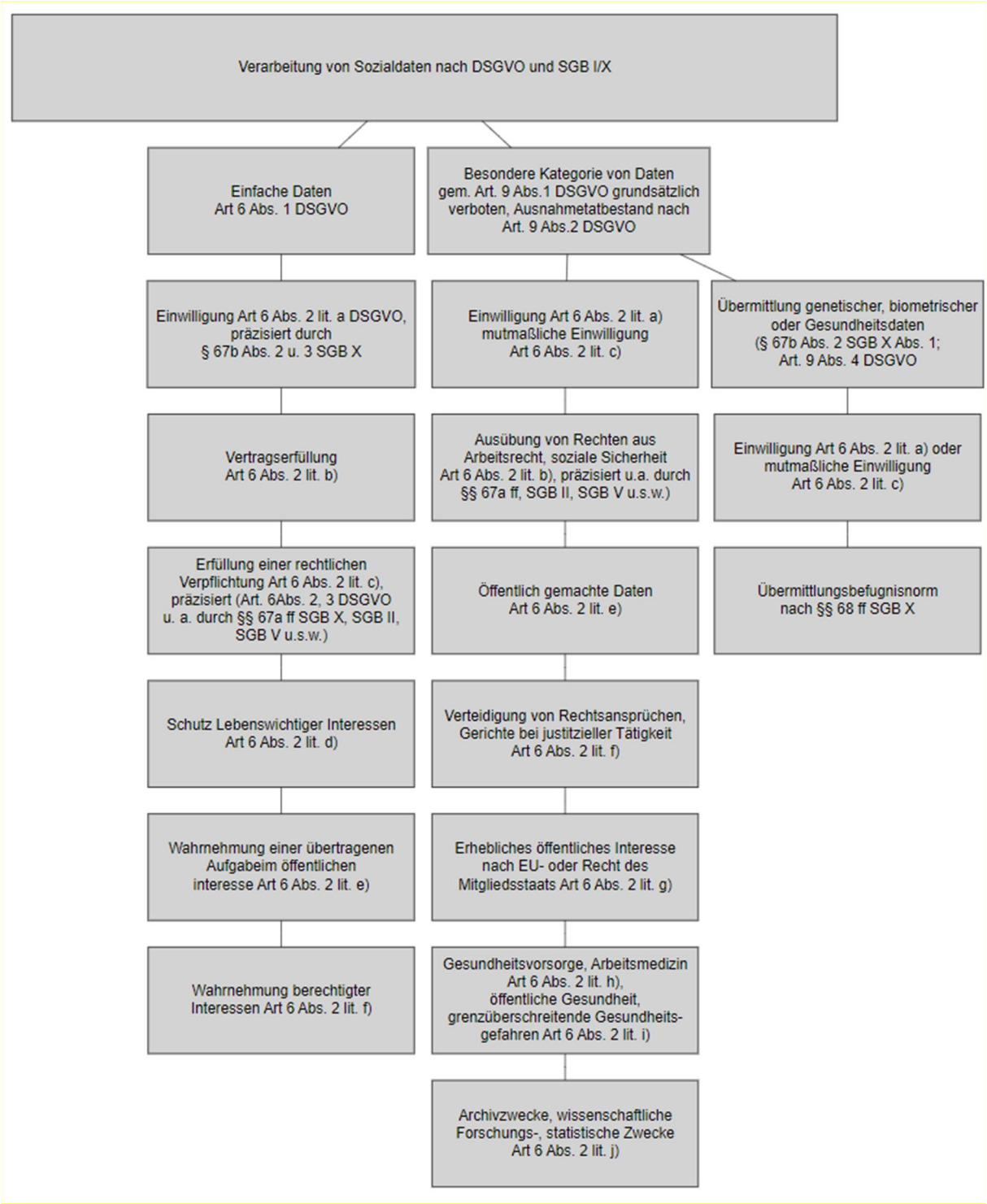

Abbildung 2 Quelle: In Anlehnung an Schaubild von Dr. Dirk Bieresborn – Richter am BSG

2.2.2 Verarbeitung von Sozialdaten zu Forschungszwecken

Die Daten dürfen nur zu dem Zweck genutzt werden, für den sie erhoben wurden. Ohne Einwilligung des Betroffenen ist eine Verarbeitung dieser Daten nur in Ausnahmefällen (z. B. Art. 6 Abs. 4 DSGVO) zulässig. Gilt eine Einwilligung als rechtlich ungültig, ist ein Nachschieben des Erlaubnistatbestands der berechtigten Interessen in der Regel unzulässig. Eine Ausnahme kann bestehen, wenn der Verantwortliche zwingend schutzwürdige Gründe für die Verarbeitung nachweisen kann. Zu Forschungszwecken ist eine Nutzung gem. § 75 SGB X möglich. Hierzu ist die Erlaubnis der Aufsichtsbehörde einzuholen. Weiter befindet sich ein Forschungsdatenzentrum Gesundheit im Aufbau (§§ 303a und 303d SGB V).

Die ärztliche Schweigepflicht ist bei der Übermittlung neben den datenschutzrechtlichen Bestimmungen zu beachten. Deshalb ist stets zu prüfen, ob die datenschutzrechtliche Verarbeitungsgrundlage gleichzeitig die Offenbarungsbefugnis i. S. d. Strafrechtsnorm ist, oder ob zusätzlich eine Entbindung von der Schweigepflicht einzuholen ist.

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 neue Pflichten mit sich. Die Etablierung eines praktikablen Verfahrens, um DSGVO-konform auf Ansprüche der Betroffenen reagieren zu können, ist empfehlenswert.

Die Rechte der betroffenen Personen sind grundsätzlich 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[21]

2.4 Datenschutzerklärung

Generell muss in der Datenschutzerklärung über jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgeklärt werden – etwa über die Verarbeitung der IP-Adresse, von Browser-Daten, Cookies, Webanalyse-Tools wie Google Analytics sowie Social Media Plugins (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?

[21] 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.

- 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
e) Social Plugins
f) Sonstige Daten

DSGVO-Checkliste zur Datenschutzerklärung (nach Art. 13 DSGVO)

Zwingend:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch Vertreter)
- Zweck und Rechtsgrundlage der Verarbeitung
- Falls Rechtsgrundlage der Art. 6 I 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 stellt hohe Anforderungen an die Technik und die interne Organisation des Verantwortlichen. Verantwortliche müssen nach Art. 24, 25 DSGVO geeignete technische und organisatorische Maßnahmen (TOM) treffen, um die Einhaltung der Datenschutzgrundsätze gem. Art. 5 Abs. 1 DSGVO, insbesondere die Datenminimierung (Art. 5 Abs. 1 Buchstabe c DSGVO) und die Datensicherheit (Art. 5 Abs. 1 Buchstabe f DSGVO) zu gewährleisten, den Vorgaben der DSGVO zu genügen und die Betroffenenrechte zu schützen (Datenschutz durch Technik, Art. 25 Abs. 1 DSGVO, auch „privacy by design“ genannt).

Welche Maßnahmen konkret erforderlich sind, hängt u.a. vom Stand der Technik, der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbunden Risiken für die persönlichen Rechte und Freiheiten sowie den jeweiligen Implementierungskosten ab (Art. 25, 32 DSGVO). Dabei müssen die Maßnahmen in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der verarbeiteten personenbezogenen Daten stehen. Es gilt jedoch zu beachten, dass unzureichende Schutzmaßnahmen nicht mit wirtschaftlichen Argumenten gerechtfertigt werden können. 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).

Neben der DSGVO enthält § 67a bzw. § 67 b Abs. 1 Satz 4 SGB X i. V. m. § 22 Abs. 2 BDSG eine konkretere Ausformung der erforderlichen technisch-organisatorischen Maßnahmen[22].

[22] § 64 Abs. 3 BDSG gilt nicht für SV-Träger, da kein Verweis im SGB enthalten ist. Jedoch können und sollten die Grundgedanken der Norm bei der Gestaltung von Systemen und Verfahren herangezogen werden.

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[23]. Die Aufsichtsbehörden gem. Art. 35 Abs. 4 DSGVO veröffentlichen eine Liste[24] 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.

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).

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

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.

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

[23] Abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
[24] Abrufbar unter: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html
[25] DSK-Konferenz vom 06.11.2023, S. 6 f.

2.7 Melde- und Informationspflichten bei Datenpannen

Nach § 83a SGB X i. V. m. Art. 33 DSGVO müssen grundsätzlich alle Verletzungen des Schutzes personenbezogener Daten gemeldet[26] werden, es sei denn, das Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich. Verantwortliche müssen sowohl den zuständigen Datenschutzaufsichtsbehörden als auch den Rechtsaufsichten [27] 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“[28] 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 außerdem auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

2.9 Gemeinsame Datenverarbeitung

Nach Art. 26 DSGVO ist es auch zulässig, dass mehrere verantwortliche Stellen eine Datenverarbeitung gemeinsam durchführen. In diesem Fall muss für jeden Verantwortlichen zu jeweils seiner Datenverarbeitung eine Ermächtigung oder Einwilligung vorliegen.

Wird die Verarbeitung auf eine Einwilligung gestützt, muss diese die Verarbeitung durch alle gemeinsam Verantwortlichen und auch die entsprechenden Weitergaben an den oder die anderen gemeinsam Verantwortlichen umfassen.

Den gemeinsam Verantwortlichen werden spezifische Pflichten auferlegt, die über die für jeden Verantwortlichen nach der DSGVO geltenden Pflichten hinausgehen. So muss eine Vereinbarung abgeschlossen werden, die ausweist,

- wer welche in der DSGVO geregelten Verpflichtungen - insbesondere im Hinblick auf Betroffenenrechte und Informationspflichten – erfüllt (Art. 26 Abs. 1 DSGVO) und
- wie sich die tatsächlichen Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen – eine nachvollziehbare Beschreibung des Zusammenwirkens der Rollen der Beteiligten und ihrer jeweiligen Beziehung zur betroffenen Person – darstellen (Art. 26 Abs. 2 DSGVO).

[26] Abrufbar unter https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-186ef7dce1/

[27] Datenschutzbehörden und Rechts- bzw. Fachaufsicht der SV-Träger.

[28] Abrufbar unter: https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

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).

Jeder der gemeinsam Verantwortlichen haftet nach Art. 82 Abs. 4 i. V. m. Abs. 2 Satz 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.

Fälle gemeinsamer Verantwortlichkeit können zu einer Erhöhung der Risiken für die Rechte und Freiheiten betroffener Personen führen, so dass die Durchführung einer Datenschutz-Folgenabschätzung (siehe Pkt. 2.7) geboten sein kann.

Die Schwierigkeit 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

Eine Auftragsverarbeitung kann durch öffentliche und nicht öffentliche Stellen durchgeführt werden. Im Falle von nicht öffentlichen Stellen sind die Voraussetzungen nach § 80 Abs. 3 SGB X zu erfüllen.

Die SV-Träger schließen als Verantwortliche einen Vertrag mit dem Auftragsverarbeiter[29]. Sie haben die Pflicht, dass alle Vorgaben des speziellen Sozialdatenschutzes nach § 35 SGB I i.V.m. §§ 67 ff. SGB X unter Beachtung der allgemeingültigen Regelungen des Art. 28 DSGVO wie Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz eingehalten werden.

[29] Beachte Besonderheit K(Z)V´en, bei der die empfangenen K(Z)V Verantwortliche für die ihnen zugesandten Daten wird (§ 77 Abs. 6 SGB V).

Zur Auftragsverarbeitung zählen dabei Verarbeitung von Datenverarbeitungsprozessen, die nicht innerhalb der eigen Arbeitsplatz-PC-Struktur erfolgen, sondern extern von einem Dritten vollständig, teilweise im Rahmen eines Cloud-Computings (siehe Pkt. 7.5) einschl. der damit einhergehenden Datenübermittlung oder möglicher Auslagerungen bei Backup-Sicherheitsspeicherungen vorgenommen werden. Zur Auftragsverarbeitung zählt auch die Prüfung und Wartung der verwendeten Hard- und Software zur Sicherstellung der originären Auftragsverarbeitung. 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 Pkt. 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.

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 Überwachung unter Zuhilfenahme der Datenschutz-Folgeabschätzung und –kontrolle und Erteilung von Unteraufträgen zu den elementaren Vertragsinhalten. Die zutreffenden vertraglichen Regelungen und Anforderungen an den Auftragsverarbeiter nach Art. 28 Abs. 3 DSGVO sind schriftlich niederzulegen oder in einem Dokument mit einer qualifizierten elektronischen Signatur aufzunehmen.

Mit der Anzeige des Auftrages des Verantwortlichen (§ 80 Abs. 1 Satz 2 SGB X) an die Rechts- und Aufsichtsbehörde im Sinne des § 87 Abs. 1 SGB IV i. V. m. Art. 28 DSGVO besteht für ihn 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 Behörde 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).[30]
Der Auftragsbearbeiter ist absolut nach den getroffenen vertraglichen Regelungen (Art. 28 Abs. 1 Satz 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) und unterliegt einer Kontrolle des Verantwortlichen, ob und inwieweit er seinen Pflichten nachgekommen ist. Gleichzeitig besitzt er eine Meldepflicht bei datenschutzrechtlichen Verstößen des Verantwortlichen (siehe auch Punkt 2.7). Er sollte für seine umgesetzten Aktivitäten eine eigene Dokumentation führen, um auch seiner Verantwortlichkeit im Sinne des

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

Art. 28 Abs. 10 DSGVO nachvollziehbar festzuhalten (siehe auch Punkt 2.8). Dem Verantwortlichen obliegt die Verpflichtung seiner Kontrollfunktion umfänglich nachzukommen (Art. 24 DSGVO), die zwingend vertraglich zu vereinbaren ist.

Der Vertrag zur Auftragsverarbeitung kann anhand der „Checkliste zur Prüfung AVV“ und dazu ergangenen Hinweisen „Hinweisen zur Nutzung der Checkliste Prüfung AVV“ formell und inhaltlich überprüft werden[31].

2.12 Datenschutzmanagement

Ergänzend zu den dargelegten Ausführungen empfehlen wir das Standard-Datenschutzmodell (SDM)[32] 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[33].

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
- Intervenierbarkeit.

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

[31] https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen
[32] https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html
[33] https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20180522_RdSchr_DSGVO_DSMS.pdf

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. Bereits etablierte Verfahren, die auf früheren Versionen des Leitfadens (und der darin zugrunde gelegten, teilweise außer Kraft gesetzten Vorschriften wie z. B. SigG und SigV) basieren, können nach Ansicht der Prüfdienste weiter betrieben werden.

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 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)

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

Empfohlen wird, für die Dateien der übertragenen Dokumente nur Dateiformate zu verwenden, die eine langfristige Lesbarkeit sicherstellen (TIFF bzw. PDF/A).

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 (siehe Minikommentar des BMI zu § 7 EGovG).

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) halten die Prüfdienste die Vorlage von Graustufen-Images mit allen Formatierungszeichen für ausreichend.

Die SV-Träger sollten sich an den Ergebnissen einer individuellen Risikobetrachtung orientieren, im Rahmen derer insbesondere die Gefahren des möglichen Verlustes der Beweiskraft von Graustufen-Wiedergaben mit den Folgen des größeren wirtschaftlichen Aufwandes bei der Digitalisierung in Farbe gegeneinander abzuwägen sind.

Obwohl es grundsätzlich keine eklatanten Preisunterschiede mehr zwischen Farb- und S/W-Scannern gibt - jeder Scanner beherrscht beide Verfahren - wäre jedoch erforderlich, dass der Scanner multistreamfähig ist. Das bedeutet, es werden beim Scanvorgang sowohl ein farbiges als auch ein S-/W-Image erzeugt. Während das farbige elektronisch signiert und archiviert wird, benötigt man das S-/W-Image nur für das Auslesen und die Nachbearbeitung der Daten. Dieses Image könnte nach dem Lesevorgang wieder automatisch gelöscht werden.

Zur Vermeidung einer erhöhten Netzwerkperformance wegen des Abrufs von Farbimages durch die Sachbearbeitung wäre auch eine weitere Nutzung des vorgenannten S-/W-Image möglich.

Es muss sichergestellt sein, dass die Belege urschriftgetreu gescannt werden. Dies erfordert auch, dass auf dem Original vorhandene Formatierungszeichen (z. B. Linien, Rahmen, Logos u.a.) auch auf dem signierten Image vorhanden sein müssen. Für das Auslesen der Rohdaten für die weitere maschinelle Verwendung (z. B. OCR-Lesung) kann auf diese Kriterien allerdings verzichtet werden.

Rückseiten sind beim Stapelsignaturverfahren grundsätzlich ebenfalls zu scannen. Ein automatisches Löschen leerer Rückseiten ist zulässig, sofern die Scansoftware gewährleistet, dass bereits bei einem auf der Rückseite befindlichen Zeichen (z. B. ein „Punkt“) ein automatisches Löschen ausgeschlossen ist.

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 ist sicherzustellen, dass der elektronische Eingangsstempel dem tatsächlichen Eingangsdatum des Papierdokumentes entspricht.
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.

Die Verwendung von Multi-TIFF-Dokumenten, bei denen ein aus mehreren Seiten bestehendes Dokument mit einer Elektronischen Signatur versehen wird, ist möglich. Vermieden werden sollte jedoch, mehrere unterschiedliche Dokumente mit einer einzigen Signatur zu versehen. Hierbei könnte das Problem auftreten, dass die einzelnen Dokumente unterschiedlich lange aufbewahrt werden müssen. Bei der Vernichtung eines dieser Dokumente müssten die anderen neu signiert werden.

Die Anforderungen gelten auch für über Apps erstellte Abbilder und deren Übermittlung sowie Speicherung beim SV-Träger.

3.2.1.3 Dokumentation des Scan-Vorgangs

Es besteht die Notwendigkeit festzustellen, wer das Dokument in die elektronische Form übertragen hat. Eine rechtliche Verpflichtung hierzu ergibt sich aus § 67b SGB X i. V. m. § 22 Abs. 2 Nr. 2 BDSG (siehe auch § 7 EGovG).

Die beim Scan-Vorgang erzeugten Images sind daher vom Scan-Operator zu signieren. Durch die Signierung bestätigt der Scan-Operator, dass das Original vorlag und in die elektronische Form übertragen wurde.

Der Integritätsschutz ergibt sich aus Art. 5 Abs.1 Buchst. f) DSGVO: Daten müssen gegen (un-) beabsichtigte Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt sein.

Wie bereits in Punkt 3.2.1.1 beschrieben, 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. 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:
Mit Einführung der eIDAS-Verordnung wurde die Signaturrichtlinie aufgehoben; das Signaturgesetz wurde durch das Vertrauensdienstegesetz (VDG) abgelöst, das am 29.07.2017 in Kraft getreten ist. Auch die Signaturverordnung trat zum 29.07.2017 außer Kraft. Der Gesetzgeber ging schon in der Vergangenheit (mit dem Signaturgesetz) davon aus, dass eine elektronische Signatur als Ersatz einer sonst erforderlichen körperlichen Unterschrift an einem einzelnen Dokument angebracht wird. Die entsprechenden Regelungen im SGB sehen daher vor, dass die Person, welche die Signatur auf einem Dokument anbringt, sich vor der Erzeugung der Signatur davon überzeugt, dass die Daten des zu signierenden Dokumentes integer sind. Klassischer Einsatzbereich ist der Sachbearbeiter-Arbeitsplatz (SB), 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 (z. B. AU-Meldungen) stapelweise eingescannt. Die erzeugten Images werden mit Hilfe einer Signaturanwendungskomponente an einen Scan-/Signaturarbeitsplatz übertragen, an dem der Signaturvorgang initiiert werden kann.

Der Vorteil dieses Verfahrens gegenüber dem der Einzelsignatur liegt im Zeitgewinn: Das Einscannen, Signieren und Speichern von Papierbelegen kann 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.

Die Prüfdienste empfehlen, unter Berücksichtigung von § 7 EGovG, dass der Signiervorgang grundsätzlich zeitlich und räumlich in unmittelbarem Zusammenhang mit dem Einscannen erfolgt. Die Signatur darf hierbei nur 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. Dieser hat aber vor dem Signiervorgang die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe zu prüfen. Das bedeutet, jedes Image ist visuell zu prüfen. Eine Stapelsignatur ist bei dieser Alternative nur zulässig, wenn im Signiertool eine voll umfängliche (100 v. H.) Prüfung erfolgt.

Die Stapelsignatur wird erstmals in § 41 Abs. 5 SRVwV als „Massensignatur“ beschrieben und an verschiedene Voraussetzungen gebunden.

Da beim Stapelsignaturverfahren nicht mehr jeder einzelne eingescannte Beleg vor seiner Signatur einer visuellen Kontrolle unterzogen wird, muss durch bestimmte technische und organisatorische Vorkehrungen ein mögliches Schadensrisiko minimiert werden.

Fernsignatur:
Die eIDAS-Verordnung, die unmittelbar gilt, bietet die Möglichkeit der Fernsignatur, die bisher in Deutschland nicht möglich war. Bei der Fernsignatur wird eine qualifizierte Signatur nicht mehr mit einer Signaturkarte erstellt, sondern von einem qualifizierten Vertrauensdienstanbieter im Auftrag des Sozialversicherungsträgers.

Der Vorteil des Verfahrens liegt darin, dass keine zusätzliche technische Ausstattung (Signaturkarte, Lesegerät) für das Erstellen einer qualifizierten elektronischen Signatur benötigt wird.

Die beauftragende Organisation muss dafür gegenüber dem Vertrauensdienstanbieter ihre Identität sicher nachweisen.

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.

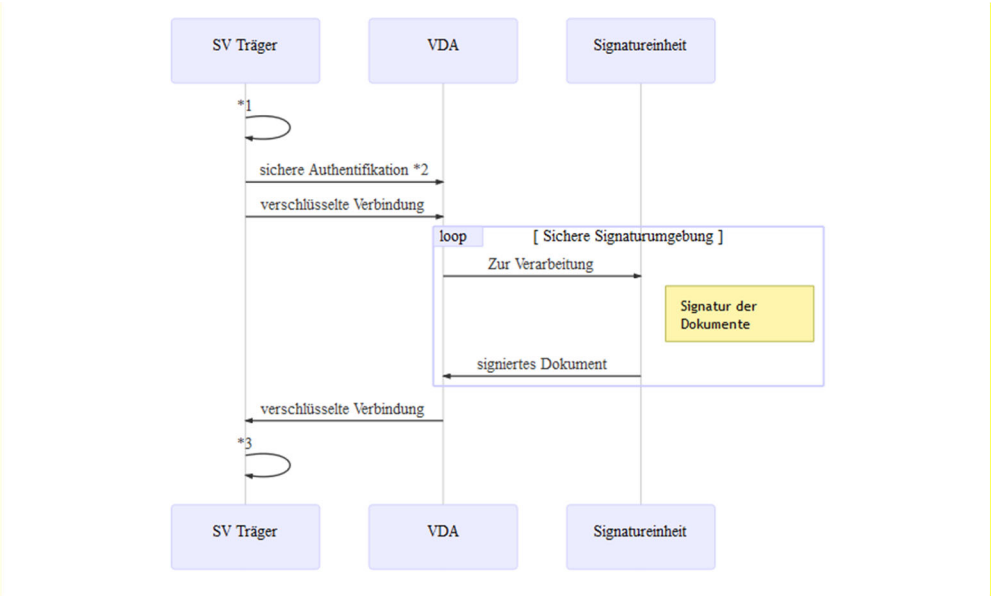

Abbildung 3 Fernsignatur

VDA = qualifizierter Vertrauensdiensteanbieter

*1 Sichtkontrolle und Scannen der Dokumente. Siehe hierzu Ausführungen im LEK Nr. 3. Nach dem Scanvorgang darf es keine Möglichkeit zur nachträglichen Bearbeitung der Dokumente geben.

*2 Entsprechend dem Schutzbedarf “Empfehlung = Schutzbedarf sehr hoch (bzw. „hoch” nach eIDAS-VO)

*3 Überführung in das Verarbeitungssystem mit Hash- / Signaturprüfung

Das oben skizzierte Vorgehen wird von den Prüfdiensten als sachgerecht betrachtet. Es ist allerdings darauf hinzuweisen, dass die eIDAS-VO keine Regelungen darüber enthält, ob das zu signierende Dokument die sicherere Umgebung zur Siegelung verlassen darf. In diesem Zusammenhang wird auf den nachfolgenden Abschnitt verwiesen.

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 insbesondere folgende Sicherheitsmaßnahmen erforderlich:

Bauliche und technische Vorkehrungen:
Bei der Gestaltung der baulichen Maßnahmen ist zu unterscheiden zwischen

- Einzelplatzsignatur und
- Stapelsignatur.

Der Einsatz von Stapelsignaturverfahren hat ausschließlich in einer abgesicherten Umgebung zu erfolgen. Die auf der Homepage der BNetzA veröffentlichten Bestätigungen zum Einsatz von Signaturanwendungskomponenten verlangen, dass der Scan- / Signatur-Bereich sich in einem geschützten Einsatzbereich befindet. Dieser darf von außen nur mit Schlüssel / Karten von Berechtigten zu öffnen sein. In diesem Bereich sind unterzubringen:

- Scanner (für die Beleglesung)
- Scan- / Signatur-Arbeitsplätze

Einzelheiten sind der Homepage der BNetzA zu entnehmen.

Die Signaturanwendungskomponente ist derart zu konfigurieren, dass die Signaturerstellungseinheit lediglich für die Signatur eines Stapels freigeschaltet wird; die Stapelgröße sollte 250 (bei Hash-Bäumen = 256) Dokumente (es werden einzelne Dokumente und nicht Seiten signiert) nicht überschreiten.

Um mangelhafte Scanvorgänge (z. B. fehlende Seiten, mangelnde Lesbarkeit) zu erkennen, muss eine geeignete Qualitätskontrolle und bei Bedarf eine erneute Erfassung des gesamten Stapels stattfinden. Die detaillierte Ausgestaltung dieser Kontrolle soll sich am Schutzbedarf der verarbeiteten Dokumente, am Scan-Durchsatz sowie an der Zuverlässigkeit des Scansystems orientieren.

Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf von „normal“ und bei hohem Durchsatz kann die Sichtkontrolle auf Stichproben reduziert werden, um systematische Fehler zu erkennen.[34] Sie sollte aber mindestens das erste und das letzte Blatt des Stapels umfassen.

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.

Für die Signatur des nächsten Stapels muss der Scan-Operator seinen Signatur-PIN erneut eingeben. Eine Freischaltung der Signaturkarte für ein festgelegtes Zeitfenster ist nicht zulässig.

Um die Übersichtlichkeit für den Scan-Operator nicht zu erschweren, sollte technisch sichergestellt sein, dass maximal ein Rückstand von drei eingescannten, ungeprüften und unsignierten Stapeln vorhanden ist.

Um die Auslastung der Scan-Signatureinheiten zu erhöhen, kann ein Scan-Operator zeitgleich zwei Scan-Straßen bedienen. Hierbei ist sicher zu stellen, dass er je Scan-Straße über eine eigene Signaturerstellungskomponente verfügt.

Vor der endgültigen Langzeitspeicherung der signierten Images im Langzeitarchiv ist jede Signatur noch einmal (automatisch) auf Gültigkeit zu überprüfen. Dies kann durch eine Online-Abfrage beim Vertrauensdienstanbieter oder gegen die auf dem Signaturserver gespeicherten (im Hause eingesetzten) Zertifikate sowie die aktualisierten Sperrlisten erfolgen.

Das Ergebnis der Überprüfung ist mit zu speichern. Sollten hierbei fehlerhafte Signaturen festgestellt werden, müssen alle nach dem Zeitpunkt der fehlerhaften Signatur eingescannten Dokumente erneut gescannt und 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).

Das Einscannen und Signieren geringer Papiermengen kann unter der Voraussetzung, dass eine Einzelsignatur an jedem Dokument angebracht wird, auch an den normalen Arbeitsplätzen erfolgen.

Darüber hinaus 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. Diese DA ist den Scan-Operatoren zur Kenntnis zu geben.

Eine Vernichtung der Papierdokumente kann nur dann vorgenommen werden, wenn die im SGB I und IV sowie der SVRV und SRVwV aufgeführten Voraussetzungen in allen Punkten erfüllt sind.

[34] 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.

Es wird empfohlen, die Vernichtung erst nach der Nachbearbeitung, z. B. Plausibilitäts- und Mitgliedschaftsprüfung, durchzuführen und wenn sichergestellt ist, dass das Dokument im Archiv vorliegt / angekommen ist.

Es muss sichergestellt sein, dass unsignierte elektronische Dokumente bei fehlenden Originalunterlagen nicht nachträglich ausgedruckt und erneut dem System (jetzt mit Signatur) zugeführt werden können.

Beim nachträglichen Scannen von Altbeständen muss das Image den bereits im System gespeicherten Informationen zugeordnet werden.

Betriebssystem und Netzwerk:
Hinsichtlich der Konfiguration und des Betriebes von Scan- / Signaturlösungen haben die Prüfdienste des Bundes und der Länder in Zusammenarbeit mit dem BSI Rahmenbedingungen definiert, die insbesondere beim Einsatz der „Stapelsignatur“ zu beachten sind:

Grundsätzlich gelten hier die gleichen Sicherheitsstandards, die auch im täglichen „Normalgeschäft“ zu beachten sind.

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. Eine „Pseudotrennung“ durch Verwendung mehrerer Netzwerkkarten im Scanclient bietet aus Sicht des BSI keine hinreichende Sicherheit.

In diesem Zusammenhang wird auf die Ausführungen zur verschlüsselten Datenübertragung innerhalb des Scansystems der TR-RESISCAN verwiesen. Werden Daten mit einem hohen Schutzbedarf verarbeitet, ist darauf zu achten, dass die Datenübertragung zwischen Scanner, Scan-Workstation, Scan-Cache und anderen damit zusammenhängenden Systemen durch geeignete Verschlüsselungsverfahren erfolgen soll. Ist dies nicht der Fall, muss ein geeigneter Nachweis erbracht werden, dass diese Kommunikationsverbindungen durch alternative Maßnahmen ausreichend geschützt sind.

Es sind nur solche Verbindungen zulässig, die von innen nach außen aufgebaut werden können. Dies ist durch eine entsprechende Hardware-Firewall sicherzustellen. Eine Anbindung dieser Arbeitsplätze an das Internet sowie den zentralen Mail-Server ist unzulässig.

Die Verwendung einer Software-Firewall auf dem jeweiligen Rechner wird für nicht ausreichend angesehen, weil Schadsoftware dazu führen kann, dass die Maßnahme wirkungslos ist.

Maßgeblich für den Betrieb der Karten sind die durch die Bundesnetzagentur (BNetzA) festgelegten Anforderungen an die Einsatzumgebung.

Dadurch ist es erforderlich, Kartenleser der Klasse 3 zu verwenden. Diese Geräte verfügen über ein Display, auf dem angezeigt wird, welche Daten vom User signiert werden.

Es sollte auf den WINS-Dienst verzichtet werden. Eine Auflösung der Rechnernamen auf IP-Adressen bzgl. Server und Mailserver sollte durch LMHOST-Eintrag sichergestellt werden.

Bei Windows-Terminal-Servern: Da das Signaturprogramm auf dem (entfernten) Server liegt, ist die PIN-Abfrage vom Terminal-PC mit einer Verschlüsselung bzw. durch den Einsatz von zugelassenen Verschlüsselungssystemen (www.bsi.bund.de) zu schützen. Maßgeblich ist, ob die Evaluierung und Bestätigung für die eingesetzte Karte den Einsatz über Terminalserver zulassen.

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.

Nicht wiederbeschreibbare Datenträger:
Die gesetzlichen Regelungen schreiben vor, dass eine elektronische Langzeitspeicherung auf Medien zu erfolgen hat, die nicht wieder beschreibbar sind.

§ 110a Abs. 2 SGB IV spricht von „dauerhaften Datenträgern“ und schränkt somit die Medienwahl nur hinsichtlich der Lebensdauer ein. Die Daten müssen während der Aufbewahrungsfristen verfügbar und jederzeit innerhalb einer angemessenen Frist wieder herstellbar sein. Somit spricht grundsätzlich auch nichts gegen die Verwendung von Tapes oder Harddisks.

Voraussetzung für die Langzeitspeicherung auf diesen Medien ist jedoch die Gewährleistung einer Versionsintegrität (WORM-Prinzip). Ein auf Harddisks langzeitarchiviertes, qualifiziert signiertes Image darf bei Aufruf durch den User nicht verändert werden (können); in diesem Fall ist automatisch eine Kopie des Images zu erzeugen, die dann unter einer neuen Versionsnummer abgespeichert wird. Hierdurch wird die Revisionssicherheit der signierten Dokumente gewährleistet. Die Möglichkeit des physikalischen Löschens nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist muss vom SV-Träger in der Dienstanweisung detailliert festgelegt werden (u. a. Zeitpunkte und Zuständigkeiten).

Fernwartung:
Aufgrund der besonderen Sicherheitsanforderungen für die technische Anbindung der im Scan-Signaturbereich eingesetzten Hard- und Software erscheint eine Fernwartung der Geräte als problematisch.

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 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. Die dreiteilige Norm hat die seit 1995 geltende DIN 32757-1 abgelöst und wird damit auch digitalen Dokumenten bzw. Datenträgern und den damit verbundenen Sicherheitserfordernissen gerecht. Ebenfalls gilt die Europäische Norm EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“. Sie enthält im Vergleich zur älteren DIN 32757-1 zwar Vorgaben für weitere Datenträger neben dem Papier, aufgrund ihrer teilweise wenig verbindlichen Formulierungen kann sie nur eingeschränkt als Maßstab herangezogen werden.

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.

Neu sind die drei Schutzklassen, die jetzt zusammen mit den Sicherheitsstufen der Klassifizierung der anfallenden Daten dienen. Bei der Ermittlung des Schutzbedarfs für die Vernichtung der Datenträger ist der Grad der Schutzbedürftigkeit dabei ausschlaggebend für die Sicherheitsstufe. Es werden insgesamt sechs unterschiedliche Materialklassifizierungen verwendet. Sie berücksichtigen auch die Größe der Informationsdarstellung auf den Datenträgern. Weiterhin werden in der DIN 66399 statt bisher fünf Sicherheitsstufen jetzt sieben definiert.

Sozialdaten sind nach derzeitiger Auffassung der Prüfdienste 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 papierhaften Faxsendungen

Fax-Sendungen, die bei dem SV-Träger auf einem „Stand-Alone-Faxgerät“ eingehen und ausgedruckt werden, müssen – sofern der Absender keine Header-Informationen mitgesandt hat – mit einem Eingangs- und Faxstempel gekennzeichnet werden. Derartige Dokumente werden von den Prüfdiensten uneingeschränkt anerkannt, sofern

- das ausgedruckte Fax archiviert wird oder
- die Ausdrucke unmittelbar nach dem Ausdruck eingescannt und das Image mit einer QES versehen im elektronischen Langzeitarchiv gespeichert werden.

Werden eingehende Papier-Faxe ausgedruckt und an eine andere Dienststelle per Fax weitergesandt, so können diese „Fax-Kopien“ bei einer Prüfung nicht anerkannt werden. Bei diesen Dokumenten ist nicht feststellbar, ob zwischen Ausdruck und „weiterfaxen“ eine bildhafte Änderung am Original-Fax vorgenommen worden ist.

Der Prüfdienst empfiehlt die Übermittlung von Unterlagen per Fax einzustellen, da Fax-Geräte sowie Übertragungswege nicht mehr den heutigen Sicherheitsanforderungen entsprechen. So sollen auch zwischen den Kunden und SV-Trägern andere Kommunikationswege aufgebaut werden.

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 Artikel 32 der DSGVO erforderlichen technischen und organisatorischen Maßnahmen sowie die Einzelheiten zur Verwendung qualifizierter elektronischer Signaturen oder sicherer IT-geschützter 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).

Zusätzliche Regelungs- und Dokumentationsbedarfe können 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 Zahlungen35 bzw. nach § 41 Abs. 1 S. 2 SRVwV beim Verzicht auf qualifizierte elektronische Signaturen ergeben[36].
Kern dieser Anforderungen ist die Erstellung einer Gefährdungsanalyse als Grundlage der in der Dienstanweisung zu regelnden Einzelmaßnahmen.

Auch neu eingeführte Verfahren und wesentliche Änderungen bestehender Verfahren müssen diesen zusätzlichen Anforderungen genügen.

In der Dienstanweisung sind Regelungen u. a. 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:[37]
- 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

---

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

[36] 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.

[37] 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

Ergonomie der Arbeitsplätze:
- Scan- / Signaturarbeitsplatz mit einem Bildschirm, auf dem das gesamte Dokument komplett abgebildet werden kann
- Schulung der Benutzer und IT-Betreuer

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. Gem. § 41 Abs. 2 SRVwV sind Attributzertifikate zwingend vorgeschrieben; durch diese wird die Verwendung der Karte auf den jeweiligen Einsatzbereich beschränkt.

Die Signaturkarten sollten in einem Bestandsverzeichnis verwaltet werden, so dass immer nachvollziehbar ist, wann welche Karten eingesetzt wurden. Außerdem können dann die Karten der Nutzer, die nicht mehr in dem jeweiligen Bereich tätig sind, gesperrt werden. Auf die besonderen Regelungen zur elektronischen Zahlungsanordnung § 40 Abs. 5 SRVwV wird hingewiesen.

Auf Grund der Abhängigkeit von den Signaturkarten könnte für jeden Nutzer eine Reservekarte vorgehalten werden (gilt insbesondere bei „Stapelsignaturbetrieb“), sofern nicht durch andere organisatorische Regelungen die Aufrechterhaltung des Scan- / Signaturbetriebes gewährleistet ist. Die Notwendigkeit sollte der SV-Träger im Rahmen einer Risikobetrachtung feststellen. Die Verwendung einer allgemein nutzbaren Reservekarte ist nicht möglich, da die Signaturkarten personenbezogen ausgestellt werden. Mit dem Trustcenter sollten vertragliche Regelungen getroffen werden, dass Ersatzkarten in vertretbarer Zeit geliefert werden können.

Signaturkarten sollten 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.

3.3.5 Langfristige Beweiserhaltung nach § 15 VDG

Neusignierung von Elektronischen Signaturen:
Elektronische Signaturen basieren auf mathematischen Komplexitätsproblemen. Der technische Fortschritt führt dazu, dass immer komplexere solcher Probleme im Laufe der Zeit gelöst werden können und somit ein Signaturalgorithmus insgesamt oder eine gegenwärtig als sicher angesehene Parametrisierung (hierzu zählt z. B. die Länge eines Schlüssels) ab einem bestimmten Zeitpunkt nicht mehr als sicher angesehen werden kann. Die elektronische Signatur verliert also durch den technischen Fortschritt im Laufe der Zeit ihre Sicherheits- und Beweiseignung, wenn nicht weitergehende Maßnahmen ergriffen werden. Insbesondere bei der Langzeitspeicherung wird sich dieser Fall häufiger ergeben.

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."
Mit der Aufhebung des Signaturgesetzes und der Signaturverordnung entfiel die bisherige gesetzliche Grundlage für den Algorithmenkatalog, der letztmals am 30.12.2016 im Bundesanzeiger veröffentlicht wurde (BNetzA, 2016). Eine Weiterentwicklung des Algorithmenkatalogs in Form eines unverbindlichen Dokuments, das die Vorgaben des Algorithmenkatalogs in Form unverbindlicher Empfehlungen zum Stand der Technik fortschreiben würde, wurde als nicht sinnvoll angesehen. Stattdessen wurde primär auf die Empfehlungen des SOG-IS-Kryptokataloges[38] (SOG-IS, 2016) verwiesen.

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. Die neu anzubringende Signatur muss dabei natürlich nicht von der Person angebracht werden, die die Ursprungssignatur erzeugt hat.

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 Übersignatur wird nicht das Dokument selbst, sondern der Hashwert signiert. Problematisch hinsichtlich des Erhalts der dauerhaften Beweiseignung ist, dass auch die Hash-Algorithmen mathematische Komplexitätsprobleme darstellen, die durch den technischen Fortschritt hinsichtlich der Sicherheit genauso beeinflusst werden, wie die elektronischen Signaturalgorithmen.

Wird ein Hashalgorithmus ab einem bestimmten Zeitpunkt nicht mehr als sicher eingestuft, so gelten auch hier die Bestimmungen aus § 15 VDG; d. h., es ist ein erneuter 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, unsicher werden, reicht es aus, den Hashwert über die archivierten Dokumente zu erzeugen, alle früheren Signaturen dabei mit einzuschließen und dann einen solchen sog. kryptografischen Zeitstempel (qualifizierte Zeitstempel der auf einer 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.

[38] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/Empfehlungen2018.pdf

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

Nehmen SV-Träger die Nachsignatur bis zu dem im SOG-IS-Katalog genannten Termin nicht 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.

Der SOG-IS-Katalog unterscheidet zwischen empfohlenen Verfahren und Legacy-Mechanismen. Die Nutzung der Legacy-Mechanismen wird nicht empfohlen, da sie nicht mehr in vollem Umfang dem kryptographischen Stand der Technik entsprechen. Ihr Einsatz genügt aber bis zu dem Zeitpunkt des Auslaufens ihrer Eignung den Anforderungen[39].

Aus der Literatur können verschiedene Empfehlungen zur Vorgehensweise entnommen werden, die auch zur Wirtschaftlichkeit der Maßnahmen beitragen. U.a. ist als eine technische Möglichkeit der Aufbau von Hashbäumen in Betracht zu ziehen (vgl. u.a. ArchiSig-Konzept).[40] Dazu muss das Dokument mit der Signatur, dem Zeitstempel sowie ggf. vorhandener Auskünfte aus dem Verzeichnisdienst exportiert werden. Daraus können die jeweiligen Archivcontainer gebildet werden (in diesem Fall ist im Container nur ein Dokument enthalten), über die dann die Hashbäume aufgebaut werden.

Als Alternative käme auch eine „große“ Containerlösung (hier sind mehrere Dokumente zusammengefasst) in Betracht, wenn eine an den Aufbewahrungsfristen orientierte Archivstruktur möglich ist.

Besonders für die langen Zeitspannen, wie sie für die Langzeitspeicherung notwendig sind, können keine verlässlichen Voraussagen der technischen Entwicklung getroffen werden.

Das Archiv sollte daher zumindest die verschiedenen Verfahren zur Neusignierung beherrschen.

[39] Siehe hierzu Abschnitt 1.1 von (SOG-IS, 2016)

[40] Roßnagel / Schmücker (Hrsg.) Beweiskräftige elektronische Archivierung, Economica Verlag, Heidelberg 2006, S. 86 ff.

4 Elektronische Kommunikation zwischen SV-Trägern und Versicherten

4.1 Grundsätze

Das zum 01.08.2013 in Kraft getretene „Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (EGovG) sieht vor, dass durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung erleichtert wird. Medienbruchfreie Prozesse vom Antrag bis zur Langzeitspeicherung sollen möglich werden.

Das EGovG präzisiert die wesentlichen Verfahrensschritte, die eine vereinfachte, aber rechtssichere, Informationsbeschaffung, Kommunikation und Antragstellung über das Internet zulassen.

Nachfolgend werden die Abschnitte aus dem EGovG dargestellt, die eine erhebliche Relevanz im Hinblick auf die Online-Kommunikation zwischen SV-Trägern und ihren Versicherten / Arbeitgebern haben. Zur Orientierung bei der Auslegung der Rechtsvorschriften können auch die Ausführungen des BMI in seinem „Minikommentar“ zum EGovG herangezogen werden.

Neben der Kommunikation über Online-Medien, gewinnt die Kommunikation über Softwareprogramme, die speziell für die Nutzung auf mobilen Endgeräten geeignet sind (sog. Apps)[41], an Bedeutung. Allgemein gelten die Aussagen / Grundsätze zur elektronischen Kommunikation über Online-Medien auch für die Apps. Dies gilt insbesondere für folgende Anforderungen, die auch beim Angebot von Apps durch die SV-Träger erfüllt sein müssen:

- Sicherer Zugang (Authentifizierung)
- Nichtveränderbarkeit / Integrität übermittelter Daten
- Einhaltung allgemeiner und spezifischer Vorgaben zu Datenschutz und Datensicherheit
- Sichere Datenwege
- Revisionssichere Speicherung / Archivierung von übermittelten Daten

In diesem Kapitel werden daher Ausführungen zu Apps aufgenommen und Hinweise gegeben, sofern hierzu besondere / spezielle 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).

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 Lang-

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

zeitspeicherung elektronisch erzeugter Dokumente. Diese sind in ihrem jeweiligen Anwendungsbereich vorrangig gegenüber den in § 7 EGovG getroffenen Regelungen zum Übertragen und Vernichten des Papieroriginals.

Nur für Behörden des Bundes / bundesunmittelbare Körperschaften geltende Regelungen:	Für Behörden des Bundes / Landes und für bundes- / landesunmittelbare Körperschaften geltende Regelungen:
§ 2 Abs. 2: Eröffnung De-Mail-Zugang	§ 2 Abs. 1: Eröffnung eines Zugangs zur elektronischen Kommunikation
	§ 3: Information über Behörden und ihre Verfahren
	§ 4: Elektronische Bezahlmöglichkeiten
	§ 5: Nachweise
§ 6: Elektronische Aktenführung	
§ 7: Übertragung und Vernichtung des Papieroriginals	
§ 8: Akteneinsicht	
§ 9: Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand	
§ 11: Gemeinsame Verfahren	
	§ 12: Anforderungen an das Bereitstellen von Daten
	§ 13: Elektronische Formulare
	§ 14: Georeferenzierung
	§ 15: Amtl. Mitteilungs- u. Verkündungsblätter
§ 16: Barrierefreiheit	

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.

Sofern landesunmittelbare SV-Träger diese Verfahren einführen wollen, sollten die im EGovG aufgeführten Grundlagen und Bedingungen beachtet werden. Weiterhin sollten die landesunmittelbaren SV-Träger laufend beobachten, ob einzelne Bundesländer entsprechende Vorschriften einführen.

4.1.2 Schriftformerfordernis und Ersatz der Schriftform

Nach § 126a 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 § 36 a 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 § 36 a Abs. 2a Nr. 1a und c). SGB I über

- einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes,
- eine eID-Karte nach § 12 des eID-Karte-Gesetzes oder
- 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 § 291 a SGB V oder mit der digitalen Identität nach § 291 Abs. 8 SGB V möglich.

Ferner ist Schriftformersatz möglich durch die Übermittlung einer von dem Erklärenden elektronisch signierten Erklärung an die Behörde mit der Versandart nach § 5 Absatz 5 des 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 Absatz 2 Satz 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 Pkt. 4.3.2 und Pkt. 5.2.5).

Zu elektronischen Verwaltungsakten siehe 4.2.2.4.

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.

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 sind dem Punkt 4.2.3 zu entnehmen.

Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das Übersenden per Post sind bei Einhaltung dieser Anforderungen nicht mehr erforderlich.

Hinweis:
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 barrierefreie Ausgestaltung der elektronischen Kommunikation und der Verwendung elektronischer Dokumente nach § 4 des Behindertengleichstellungsgesetzes (BGG) in angemessener Form gewährleisten.

Am 25. Mai 2019 ist die neue Fassung der Barrierefreien-Informationstechnik-Verordnung (BITV) 2.0 in Kraft getreten. Sie setzt diejenigen Vorgaben der Richtlinie (EU) 2016/2102 über die Barrierefreiheit von Websites und mobilen Anwendungen öffentlicher Stellen um, die nicht schon 2018 in das aktualisierte Behindertengleichstellungsgesetz (BGG) aufgenommen wurden. Neu ist: Die BITV 2.0 beschreibt 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).[42]

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.

In den Artikeln 5, 12, 25, 32 und 35 DSGVO finden sich grundlegende Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Die Verordnung fordert geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1). Mit dem Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 sind die Anforderungen aus der DSGVO in das SGB X eingeflossen.

---

[42] 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

Je schützenswerter die Daten sind, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte dürfen in keinem Fall Kenntnis von diesen Daten erhalten. 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).

Der BfDI hat in einer am 29.01.2019 herausgegebenen „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ hierzu einige grundsätzliche Aussagen getroffen, die die SV-Träger beachten sollten.
Nach Auffassung des BfDI unterliegen Gesundheitsdaten dem Schutzbedarf „hoch“[43]. Bei diesen ist eine Ende-zu-Ende-Verschlüsselung (§ 5 Abs. 3 Satz 3 DeMailG) zwingend notwendig. Auch das Bundesinnenministerium (BMI) weist hierauf in seinem „Minikommentar“ zum EGovG ausdrücklich hin.

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.[44] 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 (siehe Punkt 4.2.3.2 d)).

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 (vgl. Punkt 4.2.3.1 und 4.2.3.5).

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:

[43] Hier ist die Einstufung in die Schutzklasse „sehr hoch“ mit der Sicherheitsstufe „hoch“ nach eIDAS-Verordnung gleichzusetzen (siehe dazu Punkt 4.2.3.1)

[44] Richtlinie zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 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

- 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[45].

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.

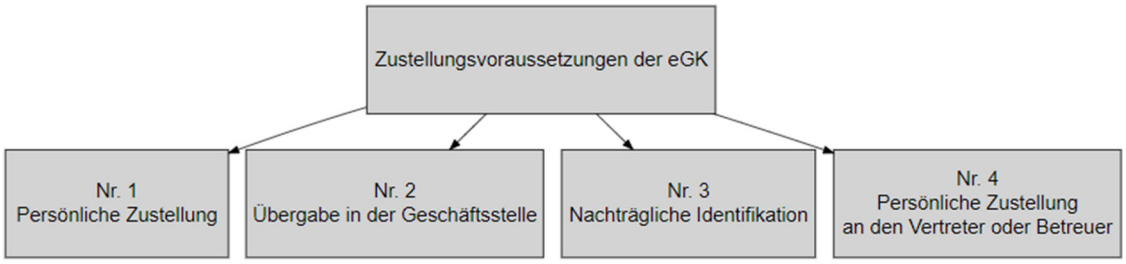

Abbildung 4 Technische und organisatorische Zustellungsvoraussetzung der eGK

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

[45] 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“.

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 LEK…Pkt. 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 (z. B. per E-Mail) erteilt haben müssen (§ 36a Abs. 1 SGB I). Die bloße Angabe einer E-Mail-Adresse reicht nicht aus. Gesundheitsdaten sind für den Versand per „einfacher“ 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 – spätestens seit 01.07.2014 – einen Zugang für die

Übermittlung elektronischer Dokumente zu schaffen hat, die auch mit einer QES 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 DS- GVO.

- Absatz 2 verpflichtet Behörden des Bundes zusätzlich, ein De-Mail-Konto im Sinne von § 5 De-Mail-Gesetz zu eröffnen. Diese Verpflichtung trifft nur die Bundesbehörden und Körperschaften, die (künftig) einen Zugang zu dem zentral im internen Verbindungsnetz des Bundes geplanten „De-Mail-Gateway“ haben.
  De-Mail-Nachrichten gelten als beim SV-Träger eingegangen, sobald sie sich im De-Mail-Postfach des SV-Trägers beim zugehörigen De-Mail-Diensteanbieter befinden.

  Eine Verpflichtung des SV-Trägers, den Versicherten auf dem De-Mail-Wege zu antworten, besteht nicht, wenn die Versicherten mehrere Zugänge gegenüber dem SV-Träger eröffnet haben. Außerdem ist der SV-Träger nicht verpflichtet, per De-Mail zu antworten. Wenn es sich um Sozialdaten mit sehr hohem Schutzbedarf handelt, sind bei elektronischen Antworten zusätzliche Sicherungsmaßnahmen (z. B. Ende-zu-Ende-Verschlüsselung) einzusetzen.

- In Absatz 3 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 bzw. § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten.

  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 b) SGB I)[46].

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.

Die Anforderungen des Onlinezugangsgesetzes (OZG)[47] sind in die Überlegungen der SV-Träger zur Gestaltung von Kommunikationsverfahren einzubeziehen. Hiernach sind spätestens bis Ende 2022 grundsätzlich alle Dienstleistungen über die entsprechenden Portale anzubieten und bestehende Portale zu einem Portalverbund zu verknüpfen.

[46] Die Voraussetzungen nach § 9a Absatz 5 des Onlinezugangsgesetzes sind gemäß § 36a Abs. 2a Nr. 1 c) SGB I zu berücksichtigen, sobald diese in Kraft getreten sind.
[47] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, BGBl. I 2017, S. 3138.
Siehe https://www.onlinezugangsgesetz.de/Webs/OZG/DE/startseite/startseite-node.html

4.2.2 Zugangsmöglichkeiten bei Schriftformersatz

4.2.2.1 Qualifizierte Elektronische Signatur

In § 36a Abs. 2 SGB I wird geregelt, dass eine durch Rechtsvorschrift angeordnete Schriftform – soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist – durch die elektronische Form ersetzt werden kann. 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 3.3.3.[48]

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)[49]. 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 zur Nutzung identifizieren (Authentifizierung – vgl. Punkt 4.2.1). 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. Artikeln 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).

---

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

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

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

Nach § 36a Abs. 2a Nr. 2. d). SGB I kann eine durch Rechtsvorschrift angeordnete Schriftform auch durch Versendung eines elektronischen Dokuments an den Versicherungsträger mit der **Versandart nach § 5 Abs. 5 DeMailG** ersetzt werden.

Der akkreditierte De-Mail-Diensteanbieter muss danach dem Nutzer ermöglichen, seine „**sichere Anmeldung**“ im Sinne von § 4 DeMailG in der Nachricht so bestätigen zu lassen, dass die Unverfälschtheit der Bestätigung jederzeit nachprüfbar ist. Um dieses dem Empfänger der Nachricht kenntlich zu machen, bestätigt der akkreditierte De-Mail-Diensteanbieter des Senders die Verwendung der sicheren Anmeldung nach § 4 durch eine QES.

Der akkreditierte De-Mail-Diensteanbieter hat zu gewährleisten, dass der Nutzer (Absender) zwischen mindestens zwei Verfahren zur sicheren Anmeldung wählen kann. Ein Verfahren muss hierbei die Nutzung der eID-Funktion des neuen Personalausweises (nPA) ermöglichen (§ 4 Abs. 2 DeMailG).

Das bedeutet:

- Bei einem bestehenden **Schriftformerfordernis** muss sich der Absender an seinem De-Mail-Konto „sicher angemeldet“ haben. Hierzu muss er für die Anmeldung zwei geeignete und voneinander unabhängige Sicherungsmittel einsetzen.
  Dies können sein:

  1. Sicherungsmittel = Benutzername und Passwort (mit weiterem Sicherungsmittel PIN)
  2. Sicherungsmittel = eID-Funktion des nPA / eGK

  Hierzu muss der Absender über die für die Nutzung der eID-Funktion des nPA erforderliche technische Ausstattung (Kartenlesegerät) und einen hierzu geeigneten Browser verfügen.

- Der De-Mail-Diensteanbieter des Absenders muss in den Metadaten der Nachricht bestätigen, dass der Absender die sichere Anmeldung gem. § 5 Abs. 5 DeMailG gewählt hat. Diese Wahl muss aus der gesendeten Mail in der Form, wie sie beim Empfänger angekommen ist, dauerhaft erkennbar sein.

- Die mit der Versandoption „absenderbestätigt“ versendete De-Mail wird automatisch mit einer QES versehen. Diese wird nicht durch den Absender selbst, sondern seinen De-Mail-Diensteanbieter angebracht. Die QES muss die Nachricht selbst, alle angehängten Dateien und die Metadaten umfassen. Durch die QES wird bestätigt, dass die Nachricht

des Absenders mit diesem Inhalt versandt wurde. Der Empfänger der Nachricht muss diese einschließlich der Metadaten und der QES archivieren. Die Form der Signierung bleibt hierbei nur solange erhalten, wie das Dokument mit der jeweiligen De-Mail-Nachricht verbunden bleibt. Die Nachricht sowie ihre Anhänge können nach dem Versand nicht unerkannt verändert werden (Integritätsschutz).

- Um die Nachprüfbarkeit der Signatur zu erhalten, dürfen auf der Empfängerseite die Nachricht und die Anhänge (z. B. PDF-Dokumente) nicht getrennt werden, sondern müssen als Ganzes aufbewahrt werden.

- Für die QES dürfen ausschließlich Zertifikate von qualifizierten Vertrauensdiensteanbietern verwendet werden. Nur diese bieten die Gewähr, dass die Signaturen dauerhaft überprüfbar bleiben.

4.2.2.4 Versand elektronischer Verwaltungsakte durch SV-Träger

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 Absatz 5 des De-Mail-Gesetzes, 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 Satz 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[50], er ist verpflichtet einen Zugang zu eröffnen (§ 2Abs. 1 EGovG)[51].

Ob der SV-Träger über den Widerspruch trotz des Formmangels der Schriftformerfordernis[52], in der Sache entscheidet, steht in seinem Ermessen. Er ist „Herr des Vorverfahrens“. Hierbei wird er zu berücksichtigen haben, ob trotz des Formmangels keine Zweifel an der Identität und Authentizität des Widerspruchs bestehen.

Zur Wahrung der Schriftform sind gem. § 36a Abs. 2a SGB I die in Punk 4.2.1 beschriebenen Verfahren möglich.

---

[50] 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
[51] siehe https://www.gesetze-im-internet.de/egovg/__2.html.
[52] Z.B. bei Widerspruchseingang in oder über eine ungesicherte einfache E-Mail.

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 vorgenannten Zugangsmöglichkeiten (Web-Portal, De-Mail) 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 / Dokumente auf andere Weise erbracht werden. Das gesamte beim SV-Träger zur Anwendung kommende Verfahren ist in einer Verfahrensbeschreibung detailliert zu dokumentieren.

4.2.3.1 Authentifizierungsverfahren - Allgemein

Bei den folgenden Ausführungen werden die Begriffe wie in der Grafik dargestellt verwandt.[53]

Abbildung 5 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

[53] Begrifflichkeiten werden entsprechend verwandt in der Richtlinie des GKV-SV zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) in der aktuellen Fassung, Punkt 2, RSchr 2021/878 abrufbar unter https://gkv-spitzenverband.de/krankenversicherung/digitalisierung/sozialdatenschutz_1/schutz_der_sozialdaten.jsp

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.

- Hierbei können insbesondere die Ausführungen des BfDI („Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“) im Hinblick auf die Übermittlung von Sozial- und Gesundheitsdaten als allgemein zu verstehende Anforderungen an die Schutzbedarfsfeststellung herangezogen werden. Dies bedeutet, dass je nach Schutzbedarf innerhalb des Portals ggf. zusätzliche Authentifizierungen für den Abruf „besonders schützenswerter“ Daten einzurichten sind.

- 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- ESISCAN“) 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

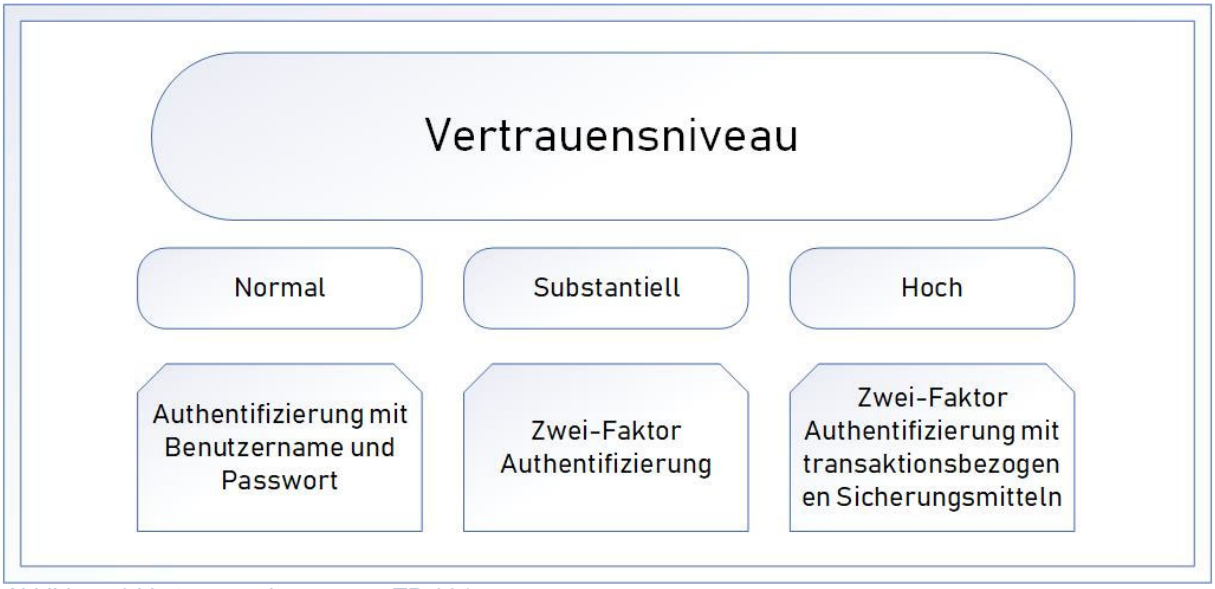

Abbildung 6 Vertrauensniveau gem. TR-03147

4.2.3.2 Anforderungen an Authentifizierung

a) Die **Mindest- oder Basisanforderung der Prüfdienste** 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.
Zu den zwei Faktoren der Authentifizierung gehören z. B. der elektronische und postalische Weg und zu den Faktoren „Besitz“ (mit Biometrie), „Wissen“.

So kann mit der Abfrage des Identifikationsmerkmals „Nutzername und Passwort“ (der Nutzername bietet erst zusammen mit dem zugehörigen Passwort die Authentifizierung) nur die Sicherheit für einen normalen Schutzbedarf erreicht werden, da der Nutzername das einzige Identitätsattribut darstellt. Die statischen Identifikationsmerkmale bieten – unabhängig von deren Zustellverfahren / Erstregistrierung (siehe d) - (alleine) keinen ausreichenden Schutz für einen höheren Schutzbedarf.

Bei der Ausgestaltung der Authentifizierungsverfahren der Träger sind auch „Geräte“ als Authentisierungsmittel (einer Person zugeordneter „Besitz“) in die Überlegungen zu einem Authentifizierungskonzept einzubeziehen (z.B. SIM-Karten; Gerätebindung).

b) Eine **höhere Sicherheit (substanzieller / hoher Schutzbedarf**; für die elektronische Übermittlung von individuellen Informationen wie persönlichen, individualisierten Daten**)** kann nur erreicht werden, wenn zusätzliche Geheimnisse wie z. B. PIN und weitere Authentifizierungsfaktoren (z. B. über Softwaretoken, Hardwaretoken) sowie kryptographische Sicherungsverfahren genutzt werden.[54]

[54] Zu „technischen“ Hinweisen siehe z. B. die Ausgabe 4/2016 der Zeitschrift „Datenschutz und Datensicherheit“ (DuD).

Dabei werden im Rahmen einer sich verändernden Authentifizierungsgrundlage[55] 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.[56]

So sind für den Schutzbedarf „hoch" transaktionsbezogene bzw. sitzungsbezogene Sicherungsmittel in sicherer Ausgestaltung in den Authentifizierungsverfahren zusätzlich zu integrieren.

Die „Zusatz-Authentifizierung" ist für eine befristete Freischaltung zur Übermittlung mehrerer Transaktionen zulässig. Der Prüfdienst empfiehlt, nach spätestens 15-minütiger Untätigkeit die Sitzung zu beenden. Eine dauerhafte Freischaltung durch einmalige Eingabe dieser „Zusatz-Authentifizierung" ist nicht zulässig.

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.

Weiterhin sind die Identifikationsmerkmale durch Verschlüsselungstechniken vor unbefugtem Zugriff zu schützen, da sie bereits selbst schutzwürdige Daten enthalten können.

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[57] .
- Die einmalige Authentifizierung am Online-Portal (Benutzername / Passwort) reicht nach Auffassung auch der Prüfdienste in keinem Fall für eine Anzeige derartiger Daten aus. Die Prüfdienste empfehlen daher ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung (qualifizierte Zwei-Faktor-Authentifizierung) vorzusehen:
  - Anmeldung mit Nutzername / Passwort **und** einem weiteren (transaktionsbezogenen oder zumindest sitzungsbezogenen) Sicherungsmittel, das mindestens z. B. ein TAN-Verfahren darstellt.

---

[55] 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.

[56] 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.

[57] Rundschreiben des Bundesversicherungsamt vom 05.09.2014 zur Sicherung des Online-Portals vor unberechtigten Zugängen und zur Verhinderung unbefugter Zugriffe auf Patientendaten im Rahmen der Patientenquittung gem. § 305 Abs. 1 SGB V sowie Rundschreiben vom 18.04.2016 zum Zugangs- und Zugriffsschutz bei digitalen Anwendungen.

- Eine sichere Authentifizierung – als an sich / allein bereits hohe Sicherheitsstufe – über
- die eID des nPA bzw. der eGK wird 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. Auf dem Markt sind bereits viele NFC-fähige Smartphones zu finden, so dass die Authentifizierung damit leichter ausgestaltet werden kann. 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.

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.

Bei der Einrichtung von SEPA-Lastschriftmandaten hat der SV-Träger als Mandatsempfänger die Beweiskraft von Mandatserteilungen sicherzustellen. Ein Schriftformerfordernis ergibt sich dabei weder aus der europäischen SEPA-Verordnung [Verordnung (EU) Nr. 260/2012] noch durch die deutsche Gesetzeslage einschließlich des SEPA-Begleitgesetzes[58]. Gleichwohl ist auch bei elektronisch erteilten Mandaten die Authentizität des Absenders und die Integrität der erhobenen Daten nachzuweisen.

Je nach Anwendungsart der Authentifizierung (Erstauthentifizierung oder Authentifizierung für den dauerhaften Zugang) und Schutzbedarfsklassifizierung der personenbezogenen Daten können z.B. folgende Verfahren benutzt werden:

- Video – Ident - Verfahren – Erstregistrierung, Sicherheitskategorie „Hoch“
- Benutzername, Passwort, mTAN – Dauerzugang, Sicherheitskategorie „Hoch“
- Fingerprint – Dauerzugang, Sicherheitskategorie „Substanziell“
- Benutzername, Passwort, per Post übermitteltes Passwort (oder QR-Code) - Erstauthentifizierung, Sicherheitskategorie „Hoch“
- Nutzung der eID-Funktion des nPA / eGK, Sicherheitskategorie „Hoch“.

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

c) Eine Authentifizierung oder Übermittlung / Änderung eines Geheimnisses als Sicherungsmittel über Telefon (Telefonzentrale) für eine anschließende Datenübermittlung sollte nicht (Empfehlung der Prüfdienste) bzw. nur bei weiterer, sicherer / zweifelsfreier Identifizierung der/des Versicherten im Rahmen des Telefonkontaktes erfolgen.[59]

[58] Beschlussempfehlung und Bericht des Finanzausschusses des Deutschen Bundestags (17. Wahlperiode Drucksache 17/11395 vom 7.11.2012).
[59] Rundschreiben des Bundesversicherungsamtes vom 18.04.2016 zum Zugangs- und Zugriffsschutz bei digitalen Anwendungen

d) Für die postalische Bereitstellung der eGK ist vor dem Versand ein Abgleich der Anschrift mit den Melderegistern durchzuführen, sofern nicht eine Authentifizierung über die in Punkt 8.2 der Richtlinie des GKV-SV nach § 217 Abs. 4b SGB V erfolgt.[60]
Die gematik hat die weitere Nutzung von Video-Ident-Verfahren für die Ausgabe von Identifizierungsmitteln zur Nutzung in der Telematikinfrastruktur (TI) (z.B. eGK) als nicht mehr zulässig erklärt und am 09.08.2022 verfügt, dass die Krankenkassen diese Verfahren aussetzen.[61]

e) Die Prüfdienste empfehlen, 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[62]:
  Bei der Erstidentifikation können verschiedene Möglichkeiten vorgesehen werden, die wiederum unterschiedlichen „Sicherheitsklassen“ (entsprechend Schutzbedarf) entsprechen können.
  Zu nennen sind z. B.
  - siehe Punkt 4.2.3.3 zur Eröffnung eines dauerhaften Zugangs
  - Identifizierungsverfahren nach BPersAG (siehe unten)

- Transaktions- oder sitzungsbezogene Authentifizierungsmittel[63]:
  Auch hierbei können Authentifizierungsmittel für unterschiedliche „Sicherheitsklassen“ vorgesehen werden, die mit steigender Sicherheit auch Zwei-Faktoren-Authentifizierungsmittel darstellen
  - TAN-Verfahren
  - TAN-Verfahren mit Nutzung weiterer sicherer Geheimnisse (z. B. zugesandte mTAN und zusätzlich eine Ziffernfolge der eGK-Kartennummer)
  - Zusendung der mTAN an ein Gerät, durch das nicht die Anforderung der mTAN erfolgte (bei mobiler Kommunikation)
  - Weitere Verfahren, die außerhalb des mTAN-Verfahrens ein weiteres Geheimnis liefern (z. B. Zugangstoken, biometrische Faktoren)

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

Mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises[64] werden mit der Ergänzung des Bundespersonalausweisgesetzes erweiterte Nutzungsmöglichkeiten der eID –

[60] Rundschreiben des GKV-SV RS 2022/026 v. 11.01.2022; Richtlinie des GKV-SV nach § 217 Abs. 4b SGB V in der aktuellen Fassung abrufbar unter: https://www.gkv-spitzenverband.de/krankenversicherung/digitalisierung/sozialdaten-schutz_1/schutz_der_sozialdaten.jsp
[61] Pressemitteilung der gematik vom 09.08.2022.
[62] Im Sinne Verknüpfung eines „Accounts“ mit einer Person / Versicherten.
[63] Authentifizierungen, die den Zugang für die Dauer der Kommunikation („Sitzung“) bzw. für eine Handlung („Transaktion“) ermöglichen.
[64] Gesetz zur Förderung des elektronischen Identitätsnachweises vom 07. Juli 2017, BGBl 2017 I, S. 2310.

Funktion des Bundespersonalausweises geschaffen. Der Bereich der Anwendungsmöglichkeiten wird dadurch über die bisherigen Möglichkeiten (z. B. Eröffnung eines Bankkontos) hinaus erweitert. Identifizierungsdienstleister (siehe § 2 Abs. 3a BPersAG n.F.) können Bestätigungen der Identität von Personen für Kunden vornehmen. Die so verifizierten Daten von Personen können dann von den Kunden (z. B. SV-Trägern) für die Authentifizierung genutzt werden (§ 19a BPersAG n.F.)
Im Rahmen der Wirtschaftlichkeitsbetrachtung sollte eingehend geprüft werden, für welche Module diese neuen Möglichkeiten bei ggf. fallzahlenmäßiger Abrechnung der Identifizierungsdienstleister genutzt werden (z. B. nur für die sichere Erstregistrierung).

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.
Das BMG prüft derzeit die Einführung alternativer Authentifizierungswege für die Telematik-Infrastruktur.

Die jeweiligen Bausteine der Erstidentifikation und der weiteren (transaktions-/sitzungsbezogenen) Identifikationsmaßnahmen sind in ihrer konkreten Schutzwirkung grundsätzlich gesondert zu betrachten. Sitzungsbezogene Merkmale (session-based) sind zulässig, sofern nach einer gewissen Zeit des Untätigbleibens der Nutzenden ein automatisches Ausloggen vorgesehen ist.

Eine Zwei-Faktor-Authentifizierung bei der Erstregistratur reicht in ihrer Wirkung nicht über das Verfahren der Erstregistratur als (grundsätzlicher) Verknüpfung der Authentifizierung mit der natürlichen Person hinaus.

Bei substanziellem / hohem Schutzniveau ist daher auch die Verknüpfung zur natürlichen Person transaktions- oder sitzungsbezogen sicher und ggf. auch im Wege einer (weiteren) Zwei-Faktor-Authentifizierung (dann transaktions-/sitzungsbezogen) festzustellen.

Dies bedeutet, je sicherer die Erstregistrierung und darüber hinaus weitere Authentifizierungsmittel bereits jeweils für sich und ihre Zwecke sind, desto sicherer ist die Kombination bzw. der modulare Aufbau bei deren kumulativer Verwendung für die entsprechende Gesamthandlung, für die die Authentifizierung erfolgt.

Bei einer Lösung, die über einen (ggf. kassenexternen) Zugang die Authentifizierung für mehrere Kassenanwendungen ermöglichen soll (sog. Single Sign-on (SSO)) reicht der Schutzbereich dieser SSO-Lösung nur insoweit, wie die Schutzbereiche / Schutzbedarfe der jeweiligen Authentifizierungsmaßnahmen dieses Punktes reichen. Auf diesen Schutzbereich kann dann jedoch durch weitere Maßnahmen aufgebaut werden.

4.2.3.3 Einbeziehung von Sicherheitseinrichtungen mobiler Endgeräte

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

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

4.2.3.4 Single-Sign-On-Verfahren

Die Authentifizierung bei einem anderen System (z.B. Bezahldienste) kann für die Authentifizierung im eigenen System des Trägers herangezogen werden (SSO). Hierbei ist zu beachten, dass – ohne weitere Authentifizierungsmittel – nur das (ggf. zu niedrige) Vertrauensniveau der ursprünglichen Authentifizierung erreicht werden kann.
Dabei ist auch zu prüfen, welche Identitätsmerkmale einer Person bzw. Zuordnungen Person / Sachverhalt bei dem anderen System überhaupt authentisiert wurden, die zur Authentifizierung herangezogen werden sollen.

In diesem Zusammenhang sind auch die Verfahren zum Zugang im Hinblick auf das OZG in die Überlegungen der Träger einzubeziehen (siehe Punkt 4.2.1).

4.2.3.5 Gültigkeitsdauer einer Authentifizierung

Konkrete Regelungen zur Gültigkeitsdauer von Authentifizierungsverfahren gibt es derzeit nicht.

Grundsätzlich sind Erstauthentifizierungen / Erstidentifikationen / Erstregistrierungen (Begrifflichkeiten siehe 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.

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

Der Antrag auf Eröffnung eines Zugangs zum Online-Portal („Online-Geschäftsstelle“) kann schriftlich oder über eine Web-Anwendung erfolgen. Die Mindestanforderung der Prüfdienste ist eine Zwei-Faktor-Authentifizierung. Die Beantragung kann folgendermaßen ausgestaltet werden:

Von den Versicherten sind bestimmte Daten zur „Erstidentifikation“ (Registrierung) abzufordern. Hierzu gehören mindestens:

- Name, Vorname

- Geburtsdatum
- eindeutiges Identifizierungsmerkmal, z. B. KV-Nummer (Sicherer wäre z. B. die Abfrage von Teilen der eGK-Kartenkennnummer (ICCSN))

Optional können an dieser Stelle bereits auch schon folgende Daten (für die spätere Nutzung des Online-Portals) von den Nutzern eingegeben werden, z. B.:

- Benutzername
- Passwort
- E-Mail-Adresse
- Mobilfunknummer

Nach Absendung der Daten erfolgt ein Abgleich der eingegebenen Mindestdaten mit den im Bestand des SV-Trägers vorhandenen Daten. Die optional bereits angegebene E-Mail- Adresse kann - nach Abgleich mit den beim SV-Träger ggf. bereits bekannten Daten - durch Zusendung einer E-Mail mit einem „Verifizierungslink“ geprüft werden.

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).

4.2.3.6.1 Nutzung der biometrischen Daten

Anstatt eines Passworts (mit den o. g. Anforderungen), das vom Nutzer festgelegt wird, können auch biometrische Daten des Nutzers für den dauerhaften Zugang zu einem Online-Portal genutzt werden.

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.

Weiterhin soll das biometrische Verfahren folgenden Anforderungen genügen:

- Die aufgenommenen biometrischen Daten / Merkmale sollen lokal (auf dem Smartphone oder Rechner der Nutzerin / des Nutzers) in einem gesicherten Bereich kryptographisch verschlüsselt und gespeichert werden. Der SV-Träger darf auf die biometrischen Merkmale der Nutzerin / des Nutzers nicht zugreifen.
- Bei der Aufnahme von biometrischen Daten müssen typische Merkmale eines langfristig stabilen physiologischen Charakteristikums (z. B. sog. Minuzien der Papillarleisten bei einem Fingerabdruck) für die spätere Verifikation extrahiert werden. Ein einfaches digitales Bild des Körpermerkmals ist für eine Verifikation nicht ausreichend.
- Zusätzlich zum biometrischen Abgleich muss eine sog. Lebenderkennung bei jeder Anmeldung durchgeführt werden. Der „Life-Test“ soll erkennen, ob die jeweiligen biometrischen Merkmale von einer lebenden Person und nicht von einer Kopie oder einem Abbild stammen.
- Neben der Anmeldung mittels eines biometrischen Charakteristikums soll auch eine Anmeldungsmöglichkeit mit einem Passwort geschaffen werden. Bei mehrmals fehlgeschlagener Anmeldung (max. 5 Fehlversuche) mit einem biometrischen Charakteristikum soll weiter nur die Möglichkeit der Anmeldung mit dem Passwort bestehen. Nach den weiteren fehlgeschlagenen Versuchen (max. 5) bei der Anmeldung mit dem Passwort soll der Zugang zum Online-Portal gesperrt werden.
- Die Gesichtserkennung ist von allen im Umlauf befindlichen Methoden die unsicherste. Da ein einfaches Foto ausreichen könnte, um an die persönlichen Daten im Smartphone zu gelangen, darf diese Methode für den dauerhaften Zugang zu einem Online-Portal nicht eingesetzt werden.
- Es sollte gewährleistet sein, dass Smartphones mit manipulierten Geräteberechtigungen (insb. mit Kits für „Root“ bzw. „Jailbreak“) erkannt und für die Authentifizierung nicht zugelassen werden.

4.2.3.6.2 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 eine sichere Erstregistrierung sollten folgende Anforderungen / Richtlinien erfüllt werden:[65]

- Das Verfahren muss in Echtzeit und ohne Unterbrechung erfolgen. In Bezug auf Integrität und Vertraulichkeit ist für die Kommunikation nur eine Ende-zu-Ende-Verschlüsselung zulässig.
- Die zu identifizierende Person hat zu Beginn einer Videoauthentifizierung / Video-Identitätsprüfung ihr ausdrückliches Einverständnis damit zu erklären, dass der gesamte Identifizierungsprozess sowie Fotos bzw. Screenshots ihrer Person und ihres Ausweisdokuments aufgezeichnet werden.
- Eine Videoauthentifizierung darf nach der Richtlinie nur von entsprechend geschulten und hierfür ausgebildeten Beschäftigten durchgeführt werden. Zu den akzeptierten Dokumenten, ihren prüfbaren Merkmalen und den entsprechenden Schulungsmaßnahmen muss eine geeignete Dokumentation vorliegen. Die Schulungen der Beschäftigten müssen in regelmäßigen Abständen (mindestens aber einmal jährlich) sowie bei Bedarf von

[65] Durch die BaFin zertifizierte Video-Ident-Verfahren sind als sehr sicher einzustufen.
Abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html

einem Dritten vorgenommen werden. Ein Bedarf kann z. B. in einer Änderung der gesetzlichen und / oder aufsichtsrechtlichen bzw. datenschutzrechtlichen Anforderungen oder im Falle eines Auftretens einer signifikanten Zahl von Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstigen Fehlern im Verfahrensablauf begründet sein.

- Die Beschäftigten müssen sich während der Identifizierung in abgetrennten Räumen und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.
- Nur Ausweisdokumente, die ausreichend fälschungssichere, im Weißlicht visuell und bei Bildübertragung mittels verfügbarer Technik ausreichend deutlich erkennbare und damit prüfbare Sicherheitsmerkmale sowie über einen maschinenlesbaren Bereich verfügen, können für die Identitätsprüfung im Rahmen eines Videoauthentifizierungsverfahrens / Video-Identitätsprüfung herangezogen werden.
- Für eine zweifelsfreie Identifizierung muss die Bild- und Tonqualität der Kommunikation in einem ausreichenden Maße gegeben sein. Ist das nicht der Fall, so muss das Video-Ident-Verfahren abgebrochen werden.
- Während einer Video-Sitzung müssen drei von insgesamt vier verschiedenen Sicherheitsmerkmalen aus verschiedenen Kategorien überprüft werden.

  Zu den optischen Sicherheitsmerkmalen zählen u.a.:

  1. beugungsoptisch wirksame Merkmale (holografische Sicherheitsmerkmale / Identigram, Hologramme, Kinematische Strukturen)
  2. Personalisierungstechnik (Laserkippbilder, Ausfüllschrift)
  3. Material (personalisierter Sicherheitsfaden, optisch variable Farben)
     Sicherheitsdruck (Mikroschrift, Guillochen-Struktur)

  Personaldokumente mit weniger Sicherheitsmerkmalen sind von dem Video-Ident-Verfahren ausgeschlossen.

- Im Rahmen des Videoauthentifizierungsverfahrens ist eine Gültigkeits- und Plausibilitätsprüfung der auf dem Ausweis enthaltenen Daten und Angaben vorzunehmen. Dies beinhaltet u. a. die Überprüfung, ob Ausstellungsdatum und Gültigkeitsdatum des Ausweisdokumentes zueinander passen.
- Ein Bestandteil der Überprüfung ist zudem eine automatisierte Berechnung der in der maschinenlesbaren Zone enthaltenen Prüfziffern sowie ein Kreuzvergleich der in ihr enthaltenen Angaben mit den Angaben im Sichtfeld des Ausweisdokumentes. Außerdem ist die Korrektheit von Ziffernorthographie, Behördenkennziffer und der verwendeten Schriftarten zu überprüfen.
- Für die Speicherung der personenbezogenen Daten bei einem Video-Ident-Verfahren gelten folgende Anforderungen des PAuswG:
  - Speicherung der Daten des Personalausweises nur in gesetzlich zulässigen Sachverhalten.
  - Speicherung der Daten durch Dienstleister, die zu Identifizierung innerhalb des Kassenverfahrens erforderlich sind.
  - Übermittlung nur der Daten an den SV-Träger, die im Trägerverfahren zur Identitätsfeststellung im Trägerverfahren erforderlich sind bzw. ggf. für die Abrechnungszwecke benötigt werden.
  - Löschung etwaiger erstellter Kopien / Ablichtungen / Screenshots / Videos des Personalausweises / personenbezogener Daten nach erfolgreicher Identifizierung der Person beim Dienstleister.
- Die zu identifizierende Person muss während der Videoübertragung eine eigens für diesen Zweck gültige, zentral generierte und von den Beschäftigten an sie (per Post, per E-

Mail oder SMS[66]) übermittelte TAN unmittelbar online eingegeben und an den Mitarbeiter elektronisch zurücksenden. Nach einem erfolgreichen systemseitigen Abgleich der TAN ist das Identifizierungsverfahren abgeschlossen.
- Aufstellung eines Schutz-Clusters (Schutzmaßnahmen) zum Video-Ident-Verfahren bzw. den verschiedenen Sicherungsmechanismen innerhalb des Verfahrens. Die Möglichkeit des Vier-Augen-Prinzips bei der Prüfung der Ausweisdokumente muss vorhanden sein. Die Aufnahmen müssen im Authentifizierungsprozess stichprobeartig geprüft werden.

Erfüllen Lösungen nicht alle o.g. Anforderungen, so ist im weiteren Verfahren der Authentifizierung (transaktions- oder sitzungsbezogen) durch ergänzende, kompensierende Maßnahmen sicherzustellen, dass eine ausreichende Absicherung gewährleistet wird.

Nach einer erfolgreichen Identifizierung müssen die vom Authentifizierungsdienstleister erhobenen authentifizierungsrelevanten Daten sicher an den SV-Träger übermittelt und verglichen werden. Nach einem erfolgreichen Matching der Authentifizierungsdaten mit den Bestandsdaten des SV-Trägers soll der Zugang zum Online-Portal eröffnet werden. Sofern der Authentifizierungsdienstleister diese Authentifizierung für weitere Registrierungen / Anmeldungen für andere Plattformen anbieten möchte, ist hierfür eine gesonderte Zustimmung des Versicherten notwendig.

Zusätzlich müssen folgende datenschutzrechtliche Anforderungen an die Trägerverfahren gelten:

- Speicherung nur der Daten aus dem Identifizierungsprozess beim SV-Träger, die für die Identifizierung (Personen oder auch Geräte) und den Nachweis der sicheren, erfolgreichen Authentifizierung sowie ggf. für die Abrechnungszwecke erforderlich sind.
- Speicherung des Merkmals im Rahmen des Registrierungsprozesses mit den bestätigten Identitätsdaten, auf welchem Wege der Authentifizierung / Feststellung der Identität erfolgt ist.
- Löschung etwaiger Kopien / Ablichtungen / Screenshots / Videos des Personalausweises / personenbezogenen Daten nach erfolgreicher Identifizierung der Person beim Dienstleister.

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.

Die Sicherheit eines Video-Ident-Produktes hängt von dem jeweiligen Gesamtverfahren, der durch das Produkt umgesetzten Anforderungen und der Einbettung in die weitere Sicherheitsinfrastruktur ab.

Zu dem Video-Ident-Verfahren sollen zusätzlich andere Möglichkeiten der sicheren Authentifizierung vom SV-Träger angeboten werden.

Am 25.04.2019 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ein Rundschreiben an die gesetzlichen Krankenkassen zur Richtlinie des GKV-SV nach § 217f SGB V veröffentlicht. In dem Schreiben wird die Auffassung vertreten, dass es zurzeit kein Video-Ident-Verfahren gebe, dass das nötige hohe Sicherheitsniveau für den dauerhaften

[66] Die Nutzung einer mTAN ist zu bedenken, denn die Handynummer kann später für die Gerätebindung als weiterem Modul der Authentifizierung genutzt werden.

Zugang zu besonders schützenswerten Daten nach Artikel 9 DSGVO gewährleisten könne. Begründet wird dies damit, dass die Verfahren durch gefälschte Ausweise angreifbar seien. Sollten die jeweiligen Gesamtkonzeptionen und der Einsatz der Video-Ident-Lösungen dem jeweiligen Stand der Technik entsprechen und für die beabsichtigten Einsatzzwecke ausreichend sicher sein (Erfüllung der wesentlichen o.g. Schutzmerkmale / Anforderungen an Video-Ident-Verfahren), können Video-Ident-Verfahren aus Sicht der Prüfdienste zur Erstregistrierung mit der Schutzstufe „Hoch“ genutzt werden.[67]

Entsprechend dem Schutzbedarf des Verfahrens, zu dem die Authentifizierung den Zugang eröffnen soll, gilt die Möglichkeit von Video-Ident-Verfahren auch für Video-Ident-Anwendungen mit besonderen, von einigen Anforderungen der genannten Richtlinie abweichenden Anwendungen (z.B. sog. asynchrone Verfahren). Diese können angewandt werden, wenn ansonsten viele Schutzmerkmale der Richtlinie im Zuge der Authentifizierung erfüllt werden.[68]

Des Weiteren existiert auf dem Markt 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.

4.2.3.7 „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.
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 jeder Mitarbeiter eines SV-

[67] Siehe auch Bestandsaufnahme des Digitalausschusses des Bundesamtes für Soziale Sicherung (Version 2.0, Stand 30.06.2020, Punkt 8.3)
https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/

[68] So auch Bestandsaufnahme des Digitalausschusses im BAS, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/sichere-identitaetsnachweise-in-digitalen-prozessen/video-ident-verfahren/

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.

4.2.3.8 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:

- Für eine Authentifizierung bei einer Online-Geschäftsstelle über eine App gelten die Ausführungen zur Online-Kommunikation.
- Bei einer Kommunikation mit dem Application-Server hat bei der Erstanmeldung zum System mindestens eine Zwei-Faktor-Authentifizierung zu erfolgen. Dies kann auf folgendem Weg geschehen:
  - Erstidentifikation am Server
  - Mitteilung der Zugangsdaten über Post
  - Die Authentifizierung am Application-Server erfolgt über die per Post mitgeteilten Geheimnisse / Zugangsdaten.
- Das zur Authentisierung genutzte Schlüsselmaterial sollte in einer sicheren Umgebung gespeichert und angewandt werden.[69]
- Bei Übermittlung von Daten der Schutzklasse „substanziell / hoch“ sind weitere (sitzungsbezogene / transaktionsbezogene) Sicherungsmittel erforderlich.
- Eine Authentifizierung des mobilen Gerätes und der Ausschluss der Kommunikation mit anderen Geräten als dem authentifizierten 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 Mindestanforderungen für alle Fälle der App-Kommunikation sind:

- 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.

[69] Die SV-Träger sollten vorab festlegen, was als sicher angesehen wird:
- Versionen der Handys
- Sandbox
- Konzept
- Updates
- Weiterentwicklungsverfahren

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. Für Daten mit einem normalen Schutzbedarf ist eine TLS-Verschlüsselung ausreichend.[70] 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 Angben. 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.[71] 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.

[70] Derzeitiger Stand der Technik ist die TLS-Verschlüsselung 1.2 und 1.3.

[71] Siehe „Empfehlungen zur Protokollierung in zentralen IT-Verfahren der gesetzlichen Krankenversicherung“. DSK vom 19.03.2010.

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-Verordnung
- Automatische Anbringung einer PGP-Signatur, die mit einem ausreichend sicheren Schlüssel erzeugt wurde

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.

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.

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.[72]

Als Mindestanforderung an die Sicherung der Übermittlungswege ist die Absicherung der Kommunikationsverbindung App / Back-End 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.

4.4 Elektronische Einreichung von Nachweisen

4.4.1 Einreichung durch die Versicherten

Nach § 5 Abs. 1 EGovG können vorzulegende Nachweise (Dokumente, Bescheinigungen, Urkunden etc.) auch elektronisch eingereicht werden. Dabei entscheidet der SV-Träger nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist.

Von diesem Grundsatz gibt es zwei Ausnahmen:

- Eine (andere) Rechtsvorschrift bestimmt, dass die Nachweise im Original (Papierform) vorzulegen sind.
- Der SV-Träger verlangt – nach pflichtgemäßem Ermessen – für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals.

In der Verwaltungspraxis wird bereits heute häufig die Vorlage von (nicht beglaubigten) Kopien zugelassen. Nach dem Willen des Gesetzgebers soll dies zur Regel werden, wenn die Vorlage eines Originals nicht durch Rechtsvorschrift angeordnet ist oder der SV-Träger sie in Ausübung seines Verfahrensermessens (§ 21 SGB X) für bestimmte Verfahren oder im Einzelfall verlangt.

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

[72] BAS Rundschreiben vom 21.10.2021, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-59caeb0ec6/

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. 2 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 2 die Form der elektronischen Einwilligung festgelegt.

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 Nr. 1 und 2 SGB X und der DSGVO genannten Voraussetzungen erhoben werden. Die Übermittlungsbefugnis für Sozialdaten 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. 2 und 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 (vgl. 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[73]

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.

[73] Zu Papier-Faxen siehe Punkt 3.3.2.

Diese Faxe können wie folgt archiviert werden:

a) In Papierform (Ausdruck des Fax, siehe 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 Mitarbeiter 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:

- 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-Grundschutzkatalogen 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 über Portale oder Anwendungen eingehenden Mitteilungen / Nachrichten 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 eine 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

Die Prüfdienste empfehlen den SV-Trägern dringend, ihr bisheriges E-Mail-Eingangskonzept zu überarbeiten und in diesem Sinne umzustellen!

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 Mail und Anhang zu speichern.

4.5.3 Speicherung eingehender De-Mails im elektronischen Langzeitarchiv

Nachrichten mit Schriftformerfordernis:
De-Mail-Nachrichten, die mit der Versandart nach § 5 Abs. 5 DeMailG (absenderbestätigt) beim SV-Träger eingehen, sind mit einer QES des De-Mail-Dienstanbieters des Absenders versehen. Diese Nachrichten enthalten außerdem die Daten der „sicheren Anmeldung“ als Metadaten. Die Nachricht ist zusammen mit den Metadaten und der QES im elektronischen Langzeitarchiv des SV-Trägers zu speichern. Das Anbringen einer neuen „Eingangssignatur“ durch den SV-Träger ist nicht erforderlich.

Es wird ausdrücklich darauf hingewiesen, dass die durch den De-Mail-Dienstanbieter angebrachte QES ausschließlich dem Integritätsschutz des Dokumentes dient.

Nachrichten ohne Schriftformerfordernis:
Diese müssen gem. DeMailG keine Absenderbestätigung und somit auch keine QES enthalten. Der Absender muss zur Erstellung auch keine „sichere Anmeldung“ am De-Mail-Account wählen.
Um der geltenden Archivierungspflicht gem. § 110a SGB IV zu genügen, sollten die SV-Träger diese De-Mail-Nachrichten (einschließlich etwaiger Metadaten) mit einer serverbasierten Eingangssignatur (QES) oder einem in Punkt 4.3.2 aufgeführten alternativen Sicherungsmittel versehen und im Langzeitarchiv speichern.

Es wird ausdrücklich darauf hingewiesen, dass diese Sicherungsmittel ausschließlich dem Integritätsschutz des Dokumentes dienen.

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 (VA) z. B. auch mündlich erfolgen (siehe § 33 Abs. 2 Satz 1 SGB X). Es müssen lediglich die in § 33 Abs. 3 Satz 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 VA die Schriftform angeordnet ist. In diesem Fall sind die in § 33 Abs. 3 bis 5 SGB X genannten Voraussetzungen zu erfüllen.

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[74] hat der SV-Träger unbedingt darauf zu achten, dass diese Mail keine personenbezogenen Daten / Sozialdaten enthält. Verwiesen wird auf die Orientierungshilfe der DSK zu den Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail vom 16. Juni 2021.[75]

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

4.6.3 De-Mails (ohne / mit Anhang)

De-Mails, die schriftformersetzende Inhalte haben, müssen vom SV-Träger über eine „sichere Anmeldung“ und die Versandart nach § 5 Abs. 5 DeMailG versendet werden. Diese De-Mails werden vom De-Mail-Diensteanbieter des SV-Trägers mit einer QES versehen.

[74] Unverschlüsselt oder nicht authentifiziert
[75] Abrufbar unter: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

Bei Verwaltungsakten muss gem. § 33 Abs. 3 Satz 3 SGB X die Bestätigung nach § 5 Abs. 5 DeMailG die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.

Bei der vom De-Mail-Diensteanbieter automatisiert angebrachten QES handelt es sich nicht um eine Willenserklärung des Absenders, hat also keine die Schriftform / Unterschrift der Absendenden ersetzende Wirkung. Diese QES ist jedoch als Integritätsschutz für das Dokument ausreichend. Eine revisionssichere Speicherung mit einem zusätzlich angebrachten Integritätsschutz (Signatur) ist möglich.

Für De-Mails ohne schriftformersetzende Inhalte gilt die Regelung zu Punkt 4.5.2.

4.6.4 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 Satz 3 SGB IV ist 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.[76] Weitere Ausführungen enthält auch die Bestandsaufnahme des Digitalausschusses des Bundesamtes für Soziale Sicherung unter Beteiligung des Prüfdienstes .[77]

Siehe zur Präsenz von Trägern auf entsprechenden Plattformen unter Punkt 8.3.

[76] Abrufbar unter https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Datenschutz_Datensicherheit/2017-08-18_Rundschreiben_SozNetze_MessagingDienste.pdf

[77] 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 Punkten 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:

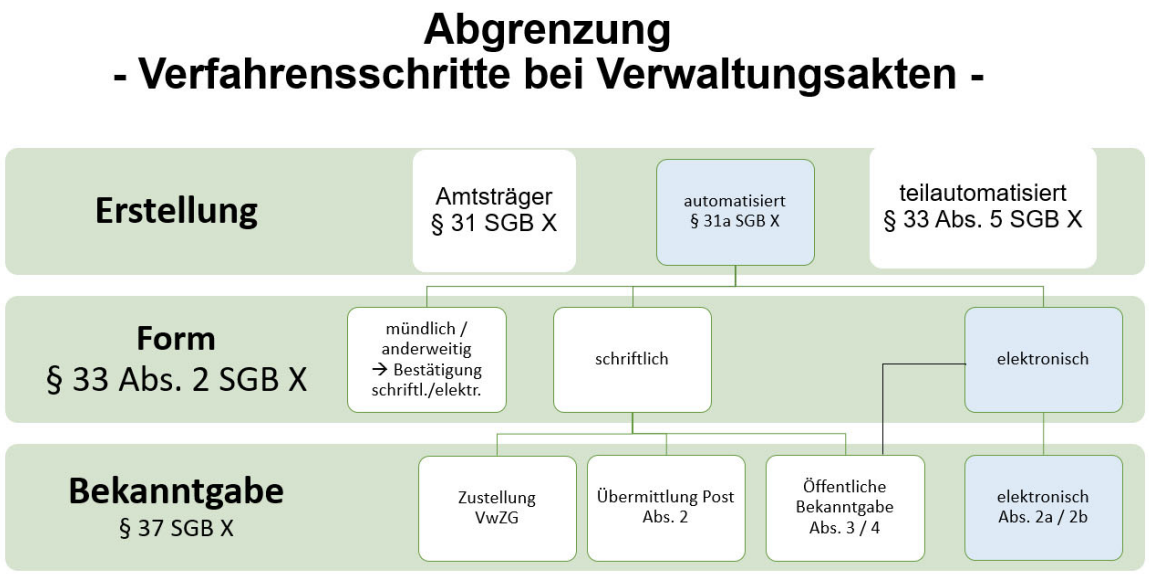

Abbildung 7 Übersicht Formen Verwaltungsakt

- **§ 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 das Greifen 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, 2a bzw. 2b SGB X[78] 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.[79]

  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.[80] 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 Verwaltungsakten; 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[81]

[78] 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.
[79] Datenschutzrechtlich bleibt der Träger verantwortlich, eine „Auslagerung“ der Verantwortung für Verarbeitungsschritte in die Sphäre der Versicherten erfolgt nicht.
[80] Siehe Digitalausschuss im BAS abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/digitaler-kundenservice-und-automatisierte-bearbeitung/bekanntgabe-eines-verwaltungsakts/
[81] In der Gesetzesbegründung wird als sicherer Benachrichtigungsweg die De-Mail nach § 5 Abs. 5 De-Mail-Gesetz empfohlen, BT-Drs. 18 / 8434, S. 121). Mit Versand der De-Mail wären dann gleichzeitig der Eingangsnachweis der Benachrichtigung und damit die Bekanntgabe verbunden.

- sichere Authentisierung Adressaten bei Zugriff auf das Portal / Online-Geschäftsstelle / App
  Für den Zugriff auf das Portal / Online-Geschäftsstelle / App sind insbesondere 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 AdressatIn in deren EDV-Systemen in gängigen Dateiformaten
- Protokollierbarkeit des erstmaligen Abrufs des Verwaltungsakts vom Portal
- Empfohlen: Aufbau eines Verfahrens, um nach Abs 2a Satz 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 AdressatIn 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 des / der AdressatIn 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 Sozialversicherungs-Rechnungsverordnung (SVRV) und der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (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. [82]
  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

[82] 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 Kapitel 5.3.1 wird hingewiesen.

Anwendung (Ausfallsicherheit, Arbeitsfähigkeit etc.) zu betrachten. Siehe hierzu auch die Ausführungen zu Punkt 4.4.1.

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

- 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 sein 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.[83] 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.

[83] Siehe Ausführungen im Abschnitt 1

5.2.6 Langzeitspeicherung

Nach Punkt 2.6 der Grundsätze ordnungsgemäßer Aufbewahrung gem. § 110a SGB IV[84] müssen - sofern Software zur automatisierten Sachbearbeitung eingesetzt wird - die durch 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.[85] 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“).

---

[84] 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 44.0. 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

[85] Organisationskonzept elektronische Verwaltungsarbeit: https://www.verwaltung-innovativ.de/DE/Verwaltungsdigitalisierung/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html.

5.3 Zahlungs- und Rechnungslegung

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 treten, die die entsprechenden Risiken minimieren (§ 40 SRVwV, Anlage 9 zur SRVwV).[86] 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.[87] 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.[88] 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 nachvollziebar (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

[86] 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).
[87] Elfte Allgemeine Verwaltungsvorschrift zur Änderung der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung
[88] Siehe Rundschreiben des BAS vom 22.06.2020, abrufbar unter:
https://www.bundesamtsozialesicherung.de/de/service/rundschreiben/detail/default-78afa2ef60/

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.[89]

5.3.2 Digitalisierung bei Abrechnungs- und Verordnungsprüfung

Voraussetzung der Digitalisierung von Originalbelegen ist zunächst die Einhaltung der Anforderungen an (Scan-)Verfahren (siehe Punkt 3. dieses Leitfadens). 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:[90]

- 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.

[89] Siehe Digitalausschuss des BAS, abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/digitalisierung-im-rechnungswesen/entwerten-digitaler-belege/
[90] Bestandsaufnahme des Digitalausschuss im BAS (Stand 30.06.2020).

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 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 § 7 Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, EGovG Bund), 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 (AT) 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.[91] Um die Anforderungen an eine Anerkennung der durch die

[91] Beschluss ist abrufbar unter:
https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Aufsichtsbehoerdentagung/20230609Protokoll_102_AT.pdf

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.
- 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.

5.4 Maschinelles Lernen und Anwendungen der Künstlichen Intelligenz

Maschinelles Lernen und Anwendungen der Künstlichen Intelligenz werden bereits in verschiedenen Arbeitsbereichen bei den Sozialversicherungsträgern 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. Die Europäische Union hat hierzu im Dezember 2023 eine Einigung über eine KI-Verordnung (AI Act) erzielt. Der Gesetzestext wurde am 13. März 2024 verabschiedet.

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 der Kapitel 1 „Planung, Vorgehen, Gestaltung der Verfahren“ sowie Kapitel 2 „Datenschutz“ dieses Leitfadens.

5.4.1 Begriffe

Der Begriff der Künstlichen Intelligenz ist weit gefasst. In Artikel 3 Nr. 1 sowie im Anhang I der KI-Verordnung wird u. a. auf folgende Techniken verwiesen:

Wenn eine Software

- Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und verstärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning);
- Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Inferenz- und Deduktionsmaschinen, Schlussfolgerungs- und Expertensysteme oder
- Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden

nutzt, und

- Ziele, die vom Menschen festgelegt werden, verfolgt,
- Ergebnisse oder Inhalte vorhersagt, empfiehlt oder entscheidet und
- das Umfeld, mit dem sie interagiert, beeinflusst.[92]

5.4.2 Wirtschaftlichkeit des Einsatzes

Vor dem Einsatz und der Entwicklung von KI-Anwendungen ist der anvisierte Erfolg in Bezug auf Machbarkeit - sowohl auf technische Umsetzbarkeit, als auch auf rechtliche Hindernisse - zu prüfen. Der Erfolg muss dabei im Verhältnis zum wirtschaftlichen Einsatz stehen.

5.4.3 Speicherung

Bei der Verarbeitung und Speicherung von personenbezogenen Daten sind die Grundsätze der Datenverarbeitung gem. Art. 5 DSGVO zu berücksichtigen. Ferner ist gemäß Art. 6 DSGVO eine rechtmäßige Verarbeitung personenbezogener Daten zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Dies gilt gleichermaßen bei der Verarbeitung von Trainingsdaten zur Entwicklung von KI-Modellen als auch bei der Nutzung einer Anwendung im Produktiveinsatz.

5.4.4 Erlaubnistatbestand / Aufgabennorm

Bei KI-Anwendungen muss bereits im Zeitpunkt der Modellerstellung, der Anwendung des Modells und dem nachfolgenden Trainieren der KI auf der Grundlage aktueller Daten darauf geachtet werden, dass es für jeden Prozess eine geeignete Verarbeitungsbefugnis gibt. Es muss daher für jeden Schritt eines KI-Verfahrens (Training, Anwendung, Lernphase aufgrund

[92] vgl. Artikel 3 und Anhang I Verordnung (EU) zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz)

erster Ergebnisse) eine Verarbeitungsgrundlage im Sinne einer diese Verarbeitungsschritte erfassenden Aufgabennorm geben. Die Reichweite der für Anwendungen der KI nutzbaren Daten ist dabei begrenzt durch die jeweilige Aufgabennorm. Änderungen des Zweckes der zu anderen Zwecken erhobenen Daten sind an § 67c SGB X zu messen.

Algorithmen für Maschinelles Lernen oder KI-Modelle benötigen Daten zum Lernen. Beim Trainieren des KI-Modells mit personenbezogenen historischen bzw. Echtdaten müssen darüber hinaus die weiteren datenschutzrechtliche Anforderungen beachtet bzw. umgesetzt werden. Nach Art. 5 Abs. 1 lit. A DSGVO müssen daher personenbezogene Daten transparent und in einer nachvollziehbaren Weise verarbeitet und dokumentiert werden. Bei Nutzung von Dienstleistern sind die Anforderungen an die Auftragsverarbeitung nach § 80 SGB X zu beachten; bei Übermittlungen und Verarbeitung von Daten an Auftragnehmer ist auch § 80 Abs. 2 SGB X (und damit auch § 77 SGB X) zu beachten.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württembergs hat ein Diskussionspapier zum Einsatz von KI auf seiner Homepage veröffentlicht.[93] Dieses Dokument soll verantwortlichen Stellen dabei helfen, sich mit den Rechtsgrundlagen auseinandersetzen, die das Datenschutzrecht für den Einsatz von Systemen der KI vorsieht. Die Inhalte des Diskussionspapieres bieten auch über die Landesgrenzen von Baden-Württemberg hinaus eine hilfreiche Perspektive für die notwendige Bewertung von datenschutzrechtlichen Aspekten beim Einsatz der KI. Eine Kurz-Checkliste zur Verarbeitung und Speicherung von personenbezogenen Daten schließt dieses Dokument ab.

Des Weiteren hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit eine Checkliste LLm-basierter (LLM = Large Language Modell) Chatbots bereitgestellt, die Behörden als Leitfaden zur datenschutzkonformen Nutzung von Chatbots dienen soll.[94]

5.4.5 Fachliche Anforderungen

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 Artikel 6 des AI Acts 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.

Für Hochrisiko-KI-Systeme ist ein kontinuierlicher Risikomanagementsystem-Prozess einzurichten. 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.

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

[93] Abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/
[94] Abrufbar unter: https://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbot

5.4.6 Technische Anforderungen

Insbesondere bei Nutzung von Clouddiensten ist eine Risikobewertung durchzuführen. Einzubeziehen sind dabei folgende technische Möglichkeiten:
Verschlüsselungsmaßnahmen (Schlüssel möglichst bei Kunden)
Einrichtung einer sog. Customer-Lockbox und damit ausdrückliche Erteilung von Zugriffen des Speicherdienstes für Supportmaßnahmen durch die übermittelnde Stelle
technischen Möglichkeiten sog. Confidential Computing. Daten befinden sich dabei in einem sog. gekapselten System bzw. in hardwarebasierten, sicheren Enklaven, sog. „Trusted Execution Environments“ (TEEs) ohne Zugriff des Betreibers des Cloud-Dienstes
geografische Beschränkung Verarbeitung auf EU/EWR.

6 Elektronischer Datenaustausch

Der Austausch von Daten zwischen SV-Trägern und deren Partnern erfolgt in zunehmendem Umfang auf elektronischem Wege. Die Richtlinien der Spitzenverbände der Krankenkassen zum Datenaustausch sind grundsätzlich geeignet, einen sicheren Datentransfer zu gewährleisten. Danach ist die Identität des Absenders und die Authentizität der Daten sichergestellt.

Die in den Datensätzen enthaltenen Informationen werden häufig in verschiedene Datenbanken übernommen. Der Originaldatensatz als adäquates Gegenstück zum papiergebundenen Dokument (z. B. Originalrechnung) wird in der Regel nicht gespeichert bzw. nicht dauerhaft und unveränderbar gespeichert. Insbesondere erfordern es die RSA-Prüfungen, dass die Krankenkassen den Informationsstand zum Zeitpunkt der Abgabe der amtlichen Meldungen nachweisen können.

Bei einem papiergebundenen Dokument kann der Inhalt und der Zeitpunkt des Eingangs zweifelsfrei ermittelt werden. Bei einem Datensatz ist dies in der Regel nicht sichergestellt. Theoretisch könnte er noch unmittelbar vor der Einsichtnahme angepasst worden sein. Damit geht die Beweiskraft der Information verloren.

Um den Nachweis der Datenintegrität erbringen zu können, 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[95] 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 zu speichern haben. Hierzu sind geeignete Archivsysteme zu nutzen, die eine Versionsintegrität gewährleisten (siehe hierzu Ausführungen zu nicht wieder beschreibbaren Datenträger unter Punkt 3.2.3). Der SV-Träger muss im Zweifelsfall den Nachweis erbringen, dass die Ursprungsdatensätze im Original vorliegen und nicht verändert wurden.

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

[95] § 110c SGB IV bzw. Heranziehung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

Bund und die Länder geltenden Haushaltsrechts vorzunehmen. Diese 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.

Die Informationen können über die Internetseiten des GKV-Spitzenverbandes heruntergeladen werden (www.gkv-datenaustausch.de). 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. 3 a SGB V).

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 Satz 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.

Ergänzend fordern § 9 Abs.1 und 3 SRVwV, dass

- die Belege zu nummerieren und geordnet und sicher aufzubewahren sind. Bei elektronisch erzeugten Dateien oder **Datensätzen** muss insbesondere sichergestellt sein, dass die Daten **verfügbar** sind und innerhalb angemessener Frist **lesbar gemacht** und **ausgedruckt** werden können. Mehrausfertigungen von Belegen müssen als solche erkennbar sein und
- Berichtigungsbuchungen sind auf dem ursprünglichen Beleg zu vermerken und durch einen neuen Beleg zu begründen; sie brauchen auf dem ursprünglichen Beleg nicht vermerkt zu werden, wenn in der Kassenordnung ein gleichwertiges Verfahren vorgesehen ist.

In § 12 Abs. 2 SRVwV ist geregelt, dass Änderungen in den zahlungsbegründenden Unterlagen so auszuführen sind, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen.

Eine Speicherung des verschlüsselten Original-Datensatzes birgt die Gefahr, dass der ursprüngliche Verschlüsselungsalgorithmus zu einem späteren Prüfzeitpunkt nicht mehr zur Verfügung steht und somit ein Entschlüsseln nicht mehr möglich wird.
Es wird daher empfohlen, die Nutzdaten nach Eingang beim SV-Träger direkt nach der Entschlüsselung elektronisch zu speichern. 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 besondere 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 Satz 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, Buchungen und Aufzeichnungen sind vollständig, richtig, zeitgerecht, geordnet und nachprüfbar für einen sachverständigen Dritten vorzunehmen. Änderungen in zahlungsbegründenden Unterlagen sind so auszuführen, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen. Alle Buchungen müssen belegt sein, und Belege können auch elektronisch erzeugte Dateien oder Datensätze sein.

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 Software-Ersteller angefertigt werden, ist der Buchführungspflichtige für die Vollständigkeit und den Informationsgehalt der Verfahrensdokumentation verantwortlich.

Die Verfahrensdokumentation der Software muss gemäß Anlage 9 zu § 40 SRVwV insbesondere beinhalten:

- Beschreibung der sachlogischen Lösung
- Beschreibung der programmtechnischen Lösung
- Beschreibung, wie die Programmidentität gewahrt wird

- Datenintegrität
- Arbeitsanweisungen für den Anwender
- Rollen- und Berechtigungskonzept zu den relevanten Zahlungsfunktionen
- Risikoanalyse
- Ordnungsmäßigkeitskonzept

Beschreibung der sachlogischen Lösung: Die sachlogische Beschreibung enthält die Darstellung der fachlichen Aufgabe aus der Sicht des Anwenders.

Diese soll folgende Punkte enthalten:

- Generelle Aufgabenerstellung
- Beschreibung der Anwenderoberflächen für Ein- und Ausgabe einschließlich der manuellen Arbeiten
- Beschreibung der Datenbestände
- Beschreibung von Verarbeitungsregeln
- Beschreibung des Datenaustausches
- Beschreibung der maschinellen und manuellen Kontrollen
- Beschreibung der Fehlermeldungen und der sich aus Fehlern ergebenden Maßnahmen
- Schlüsselverzeichnisse
- Schnittstellen zu anderen Systemen

Beschreibung der programmtechnischen Lösung: Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programm umgesetzt werden.

Beschreibung, wie die Programmidentität gewahrt wird: In der Beschreibung, wie die Programmidentität gewahrt wird, hat der Buchführungspflichtige nachzuweisen, dass die sachlogischen Forderungen durch die eingesetzten Programme erbracht werden bzw. erbracht worden sind. Hierzu gehören die präzise Beschreibung des Freigabeverfahrens mit Regelungen über Freigabekompetenzen, der durchzuführenden Testläufe und die dabei zu verwendenden Daten sowie Anweisungen für Programmkontrollen.

Datenintegrität: (siehe dazu Punkt 5.2.5)

Arbeitsanweisungen für die Anwender: Die Arbeitsanweisungen, die für den Anwender zur sachgerechten Erledigung und Durchführung seiner Aufgaben vorhanden sein müssen, gehören ebenfalls zur Verfahrensdokumentationen und sind schriftlich zu fixieren. Das ist insbesondere die Beschreibung der im Verfahren vorgesehenen manuellen Kontrollen und Abstimmungen. Die Schnittstellen zu vor- und nachgelagerten Systemen sind hierfür zu berücksichtigen.

Rollen- und Berechtigungskonzept für die Zahlungsfunktionen: Zur Abbildung des Vier-Augen-Prinzips und zur Bestätigung der sachlichen und rechnerischen Richtigkeit können Funktionen der eingesetzten Anwendungssysteme verwendet werden, soweit es hierfür ein differenziertes Rollen- und Berechtigungskonzept gibt. Hierdurch wird die Abbildung der verschiedenen Rollen, z. B. durch Abgleich der zugelassenen Personen mit den entsprechenden Berechtigungsstufen, ermöglicht. Um die elektronische Bestätigung revisionssicher zu machen, sind die jeweiligen Prüf- und Verarbeitungsschritte entsprechend zu protokollieren.

Gefährdungsanalyse: In einer Gefährdungsanalyse sind die Risiken zu ermitteln und zu bewerten (siehe dazu Punkt 5.2.3). Dabei sind die durch Fehler und Missbrauch bedingten haushaltswirtschaftlichen Auswirkungen gegen die zusätzlichen Ausgaben zur Erhöhung der Verfahrenssicherheit abzuwägen.

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

Ordnungsmäßigkeitskonzept: Im Ordnungsmäßigkeitskonzept sind die Einzelheiten zur Abgrenzung der Verantwortlichkeiten (Berechtigungskonzept) und die nachfolgenden Maßnahmen darzustellen. Es ist zu bestimmen, ob und inwieweit
- zwei oder mehr Personen maßgeblich an einem einzelnen Geschäftsvorfall zu beteiligen sind,
- nur eine Person den Geschäftsvorfall bearbeitet,
- eine Anordnung zusätzlich von einer weiteren Person zu prüfen und freizugeben ist,
- vollautomatisierte Verfahrensabläufe ohne Beteiligung einer Person Anwendung finden,
- zusätzliche Prüfverfahren einzusetzen sind und
- Sicherungsmaßnahmen zu treffen sind.

6.5 Interoperabilität

Das von der Gesellschaft für Telematik (gematik) gem. Art. 1 Patienten-Datenschutz-Gesetz (PDSG) in Verbindung mit § 384 SGB V aufzubauende Interoperabilitätsverzeichnis soll die Interoperabilität zwischen informationstechnischen Systemen im Gesundheitswesen fördern. Dabei soll im Sinne einer sinnvollen Nutzung ein übergeordneter Zweck des Datenaustausches impliziert sein.[96]

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 E-Mail-Datenaustauschverfahren

Im Rahmen von Datenaustauschverfahren zwischen SV-Trägern / Institutionen sind die Ausführungen zu Punkt 4.4.2 zu beachten.

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

6.8 Verfahren nach § 79 SGB X

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

6.9 Nutzung von Gesundheitsdaten

Die Nutzung von Gesundheitsdaten als personenbezogene Daten besonderer Art unterliegen besonderen Anforderungen.[97] Eine Verarbeitung ist generell nur bei Vorliegen eines Erlaubnistatbestands und einer Aufgabennorm möglich. Für Forschungszwecke ist § 75 SGBX zu beachten.

Kranken- und Pflegekassen können nach § 25b SGB V in der Fassung des GDNG eine datengestützte Erkennung individueller Gesundheitsrisiken vornehmen. Die Anforderungen an entsprechende Verfahren sehen u.a. Hinweise an die Versicherten (Abs. 1) und eine Anzeige an die Aufsichtsbehörde (Abs. 6) vor.

[97] Siehe https://www.datenschutzkonferenz-online.de/entschliessungen.html

7 Langzeitspeicherung und Löschung elektronisch erzeugter Dokumente und Daten

7.1 Langzeitspeicherung

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

Eingehende Dokumente:

- Elektronisch erzeugte Dokumente (z. B. im DOC- oder PDF-Format), die elektronisch an den SV-Träger gesandt wurden (z. B. auf Datenträger, E-Mail-Anhang, ftp)
- Eingegangene elektronische Faxe (z. B. auf Fax-Server)
- Eingegangene E-Mails, De-Mails und deren Anhänge
- Im Web-Formular auf der Internetseite des SV-Trägers erzeugte Daten im Text- oder PDF-Format

Ausgehende / erzeugte Dokumente:

- „Durchschriften“ der vom SV-Träger oder seinen Beschäftigten erzeugten elektronischen Dokumente, die elektronisch (und / oder in Papierform) an Externe versandt wurden (auch elektronische Faxe)
- Vom SV-Träger oder seinen Beschäftigten an Externe (z. B. Versicherte, Arbeitgeber, Leistungserbringer) versandte E-Mails, De-Mails und deren Anhänge
- Interne Vermerke, Verfügungen, Notizen, Protokolle

Die Anforderungen an die rechtssichere Langzeitspeicherung für diese Dokumente sind definiert durch die §§ 110a bis 110c SGB IV i. V. m. den Grundsätzen ordnungsgemäßer Aufbewahrung sowie dem EGovG.

Darüber hinaus ist die Sicherheit in der Verarbeitung gem. Art. 32 DSVGO zu beachten. Die technischen und organisatorischen Vorgaben ergeben sich aus § 67b Abs. 1 Satz 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 muss unveränderbar aufbewahrt werden.
- Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.
- Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.
- Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
- Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
- Jedes Dokument muss zeitnah wiedergefunden werden können.
- Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.

- Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

7.2 Besonderheiten

7.2.1 Aufbewahrung von Fehler- / Bearbeitungslisten

Fehler- / Bearbeitungs- / Kontrolllisten möchten viele SV-Träger nicht mehr in Papierform ablegen, sondern in elektronischer Form speichern. Sofern diese Listen in den Grundsätzen ordnungsmäßiger Aufbewahrung aufgeführt sind, müssen sie aufbewahrt werden. Ansonsten ist eine Aufbewahrung in das Ermessen des SV-Trägers gestellt; er muss entscheiden, ob der Inhalt der Listen einen „rechtserheblichen Charakter“ besitzt.

In der Papierform sind die Listen einzuscannen und mit einer QES des Scan-Operators zu versehen (Nachvollziehbarkeit wer das Dokument wann in die elektronische Form überführt hat - § 67b SGB X i.V.m. § 22 Abs. 2 BDSG). In der elektronischen Form muss die (Druck-) Datei ebenfalls mit der QES / fortgeschrittenen Signatur des Bearbeiters bzw. einem elektronischen Siegel des SV-Trägers versehen im Langzeitarchiv gespeichert werden.

7.2.2 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen

Für die in einer elektronischen Akte (eAkte) aufzubewahrenden Einzeldokumente können gem. Aufbewahrungskatalog unterschiedliche Aufbewahrungsfristen gelten. 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 Satz 2 SGB X, da die Fallakte einen Gesamtzusammenhang schafft, in dem eine Aufbewahrung zur allgemeinen Aufgabenerfüllung des SV-Trägers erforderlich sein kann.

Es gibt unterschiedliche Ausprägungen elektronischer Vorgangsbearbeitungen, dennoch wird dringend empfohlen, eine zeitnahe und vollständige Umstellung auf elektronische Akten und auf eine digitale Bearbeitung anzustreben[98]. Auf diese Weise können die Prinzipien der Datenminimierung und ggf. Auskunftsansprüche von Betroffenen praktisch wirksam und effizient umgesetzt werden.

7.3 Technische Richtlinie TR-03125 (TR-ESOR)

Das BSI hat mit der TR-03125 (TR-ESOR) ein Dokument zur Verfügung gestellt, das Orientierung und Hilfestellung gibt, um den vielfältigen Anforderungen hinsichtlich

- Verfügbarkeit und Lesbarkeit,
- Integrität und Authentizität sowie
- Datensicherheit und Datenschutz

von elektronischen Daten aller Art über lange Aufbewahrungszeiträume hinweg zu genügen. Gegenstand und Ziel der TR ist die Beweiswerterhaltung von kryptographisch signierten Dokumenten. Konkret enthält sie einen Katalog von verpflichtenden Muss-, von empfohlenen

[98] Zu Finanzämtern siehe Tätigkeitsbericht 2022 BfDI, S. 90

Soll- und von optionalen Kann-Anforderungen im Hinblick auf alle Elemente und Bereiche, in denen Gestaltungsbedarf hinsichtlich einer vertrauenswürdigen Langzeitspeicherung besteht. Die TR ist auf der Internetseite des BSI veröffentlicht.

Die Archivlösung der SV-Träger kann gegen die in der TR-ESOR aufgeführten Anforderungen geprüft und deren Konformität festgestellt werden. Dies erfolgt über vom BSI zertifizierte Bestätigungsstellen.

Bei dieser Prüfung werden alle **Muss-Anforderungen** auf ihre uneingeschränkte Umsetzung hin überprüft. Eine Abweichung von den Muss-Anforderungen ist nicht zulässig. Die Nichteinhaltung von **Soll-Anforderungen** muss durch den Antragsteller schlüssig und nachvollziehbar, schriftlich begründet werden.

Die Prüfdienste des Bundes und der Länder haben einige Inhalte der TR-ESOR im Anhang 1 zum Leitfaden dargestellt. Die Texte in der Spalte „Anforderungen“ sind aus dem Hauptdokument der TR-ESOR übernommen worden. Es sind nur die Anforderungen aufgeführt, die aufgrund entsprechender rechtlicher Vorgaben für SV-Träger von denen der TR-ESOR abweichen. Die sonstigen Grundanforderungen sind der TR-ESOR selbst zu entnehmen.

Es wird empfohlen, die im TR-ESOR-Hauptdokument und seiner Anlage B (Profilierung für Bundesbehörden) enthaltenen **Muss- und Soll-Anforderungen** hinsichtlich einer revisionssicheren Langzeitspeicherung elektronischer Dokumente zu beachten und umzusetzen. Die Empfehlung gilt auch für die Langzeitspeicherung nicht signierter Dokumente / Daten.
Die Prüfdienste des Bundes und der Länder werden die in der Anlage aufgeführten Muss- und Soll-Anforderungen bei Prüfungen der revisionssicheren Langzeitspeicherung als Prüf- und Bewertungsgrundlage heranziehen.

7.4 Löschung von Daten der elektronischen Kommunikation

Die Verpflichtung zur Löschung personenbezogener Daten ergibt sich aus
Art. 17 Abs. 1 DSGVO. Die Einhaltung dieser Verpflichtung kann ab einem gewissen Komplexitätsgrad nur durch ein detailliertes Löschkonzept[99] gewährleistet werden. Zudem müssen in einem Verfahrensverzeichnis gem. Art. 30 Abs. 1 Buchstabe f DSGVO Löschfristen spezifiziert werden.

Bei der Erstellung des Löschkonzeptes und der Löschfristen ist zu beachten, dass hierunter nicht nur Nutzdaten sondern auch Metadaten (z. B. Log-Daten zu Web-Seiten, Tracking-Daten und App-Daten) fallen.

Es wird empfohlen, die speziell für den Bereich der Online-Kommunikation geltenden Löschregeln in das Gesamtkonzept des SV-Trägers zur Löschung von Daten aufzunehmen (siehe auch 2.11 – Baustein Löschen und Vernichten).

7.5 Datenspeicherung in der Cloud

Cloud Computing kann neben der eigentlichen Speicherung von Daten auch Grundlage vieler Anwendungen sein, die aufgrund des besonderen Datenspeicherbedarfs bei der technischen

[99] Vorgaben zur Erstellung und den Inhalten eines Löschkonzeptes enthält die DIN 66398 („Leitlinie Löschkonzept“).

Verarbeitung Elemente der Cloudspeicherung integriert haben (z.B. Anwendungen zur Bereitstellung von Inhalten – Content Delivery / Distribution Networks, Anwendungen des Maschinelles Lernens und der Künstlichen Intelligenz).[100]

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

In jedem Fall ist für das 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[101]

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[102]
Bei einer Auftragsverarbeitung müssen die §§ 80 SGB X und 85 SGB IV sowie Artikel 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 technisch-organisatorische Maßnahmen in der Risikoanalyse aufgenommen und bewertet werden, die neben der eigentlichen Speicherung eine weitere Datenübermittlung bzw. Verarbeitung durch den Anbieter bzw. weitere Dienstleister (ggf. und insbesondere in unsicheren Drittstaaten, s.u.) ausschließt. Zu nennen sind an dieser Stelle verschlüsselte Übertragung (immer erforderlich) und auch eine verschlüsselte Speicherung (Schlüssel nur beim Verantwortlichen, nicht bei Cloud-Betreiber) sowie die Nutzung sog. Souveräner Clouds.[103]
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, sollte bei Vertragsschluss eine Wechselmöglichkeit zu einem anderen Anbieter oder Rückmigration auf eigene Infrastruktur („Exit-Strategie“) berücksichtigt werden.

[100] Zur (umstrittenen) Bewertung der Arbeitsgruppe der Konferenz der unabhängigen Datenschutzbehörden (DSK) zu Microsoft 365 siehe Festlegung der DSK v. 24.11.2022; die Ergebnisse der Arbeitsgruppe sollen noch weiter bewertet werden.
[101] Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2016/Anforderungskatalog-Cloud_Computing-C5.html
[102] Abrufbar unter: https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/ki-big-data-cloud-computing-und-automatisierte-bearbeitung/cloud-computing/
[103] Zur Nutzung Souveräner Clouds s. Stellungnahme der Konferenz der unabhängigen Datenschutzbehörden (DSK) v. 11.05.2023 zu „Kriterien für Souveräne Clouds“.

Datenübermittlung zu (Unter-)Auftragnehmern in anderen Staaten
Insbesondere darf ein Auftrag zur Verarbeitung von Sozialdaten gemäß § 80 Absatz 2 SGB X nur erteilt werden, wenn die Verarbeitung

- im Inland,
- in einem anderen Mitgliedstaat der Europäischen Union,
- in einem sog. gleichgestellten Staat (§ 35 Absatz 7 SGB I)
- oder in einem Drittstaat oder in einer internationalen Organisation erfolgt, sofern ein Angemessenheitsbeschluss der EU-Kommission gemäß Artikel 45 DSGVO vorliegt.

Werden z.B. für Wartungs- und Servicedienstleistungen, außerhalb der o.a. räumlichen Beschränkungen, 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.[104] 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“ 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.[105]

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) ausschließt bzw. zumindest ausreichende Schutzmaßnahmen vorsehen, die einen Zugriff aus diesen Drittstaaten heraus technisch ausschließen (z.B. Verschlüsselungskonzepte, s.o. allgemeine Anforderungen).

§ 393 SGB V
Nach § 393 SGB V in der Fassung des Digitalgesetzes (DigiG) gelten für Krankenkassen besondere technische und organisatorische Anforderungen an die Nutzung von Clouddiensten gelten. Diese Anforderungen sind vorrangig gegenüber den vorstehend genannten Anforderungen für andere Träger der Sozialversicherung nach allgemeinem Recht. Die Anforderungen einer Nutzung von Systemen nach Standard C5 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.
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

[104] Bundeskartellamt 2. Vergabekammer des Bundes vom 13.02.2023, Az. VK2-114/22.
[105] Siehe Anwendungshinweise DSK vom 04.09.2023 Abrufbar unter: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html.

im Rahmen einer Risikofolgenabschätzung und Überprüfung der Wirtschaftlichkeit herangezogen werden.

8 Onlineplattformen

Die gesetzliche Sozialversicherung befindet sich im digitalen Umbruch. Die Transformierung analoger in digitale Prozesse sowie eine Vielfalt innovativer Anwendungen verändern in rasanter Geschwindigkeit die Abläufe der beteiligten Akteure in der Sozialversicherung, sowohl im Innen- als auch Außenverhältnis. Ermöglicht und begleitet wird dieser Wandel durch verschiedene gesetzliche Vorschriften.

Ein besonderes Augenmerk gilt hierbei der Telematikinfrastruktur als zentraler Plattform für digitale Anwendungen im Gesundheitswesen, deren Gesamtverantwortung auf die eigens dafür gegründete Gesellschaft für Telematik (gematik) übertragen wurde. Grundlage dafür war § 306 SGB V; die Rahmenbedingungen sind in den weiteren Vorschriften des Elften Kapitels im SGB V definiert.

Ergänzend dazu sind Digitale Gesundheitsanwendungen (DiGAs) sowie Digitale Verwaltungsleistungen durch die Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) bzw. das Onlinezugangsgesetz (OZG) in den Fokus der SV-Träger gelangt. Im Falle der DiGA wurde eine leistungsrechtliche Grundlage geschaffen, um neben ärztlichen Behandlungen als Ergänzung zum Therapieerfolg auch mögliche Kosten einer „App auf Rezept“ zu übernehmen. Beim OZG sind bisherige Verwaltungsprozesse sukzessive auch digital über Verwaltungsportale von Bund und Ländern anzubieten.

Neben den gesetzlichen Grundlagen bzw. Verpflichtungen sind mit dem Einsatz, der Bereitstellung oder Unterstützung dieser digitalen Medien auch Maßnahmen zum Datenschutz und zur Datensicherheit verbunden. In Teilen befassen sich die Prüfdienste des Bundes und der Länder mit diesen Themen und werden sukzessive Prüfanforderungen erarbeiten und hier veröffentlichen, die als Grundlage für ein gegenseitiges Verständnis dienen soll.

Weitere Rechtsvorgaben / Hilfen / Unterlagen

- 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 zu 4.3.4)

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.
Im elften Kapitel des SGB V sind der Gesellschaft für Telematik (gematik) Aufgaben zur Sicherung der TI vorgegeben. Auf dem Markt existieren verschiedenste Anwendungen, die mit oder ohne Bezug zur eGK genutzt werden können. Gemäß § 290 Abs. 4 SGB V darf die KV-Nr. eines Versicherten im Rahmen der Telematikinfrastruktur von Anbietern und Nutzern von Anwendungen und Diensten im Sinne von § 306 Absatz 4 Satz 1 und 2 SGB V zur eindeutigen Identifikation des Versicherten verwendet werden, soweit dies für die eindeutige Zuordnung von Daten und Diensten bei der Nutzung dieser Anwendungen und Dienste erforderlich ist.

Am 26.03.2024 ist das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) in Kraft getreten. Kernpunkt des Gesetzes ist die für die gesetzlichen Krankenkassen verpflichtende Einführung der elektronischen Patientenakte (ePA). Die Vorschrift des § 342 Abs. 1 SGB V wird dahingehend geändert, dass die Krankenkassen ab dem 15.01.2025 verpflichtet werden, 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.

Gleichzeitig soll das E-Rezept besser nutzbar werden. Hierzu soll es zukünftig möglich sein, die E-Rezept-App der gematik auch mittels der ePA-Apps zu nutzen. Des Weiteren wird ermöglicht, digitale Identitäten, NFC-fähige elektronische Gesundheitskarten (eGK) sowie dazugehörige PINs aus der E-Rezept-App heraus zu beantragen. Die Kassen sollen verpflichtet werden, ihre Versicherten über das E-Rezept zu informieren.

Daneben gibt es Anwendungen in der TI, die keinen direkten oder lediglich sekundären Kassenbezug aufweisen, wie das Notfalldatenmanagement, das elektronische Rezept (e-Rezept), den elektronischen Medikationsplan (eMP) oder die Kommunikation im Medizinwesen (KIM) zur Übermittlung einer elektronischen Arbeitsunfähigkeitsbescheinigung (eAU). Die gematik ist für die Zulassung dieser Anwendungen verantwortlich. Auf ihrer Internetseite www.gematik.de stellt die gematik die jeweiligen TI-Anwendungen vor, gibt Erläuterungen zur Funktionsweise, präsentiert die jeweilige Weiterentwicklung dieser Anwendungen anhand einer Roadmap und listet in einer Übersicht die bereits zugelassenen Produkte der Krankenkassen auf.[106] Darüber hinaus bietet sie ein Glossar zur Erläuterung der Begrifflichkeiten rund um die TI an.[107]

Dienstleister, die mit der Herstellung oder Wartung eines Anschlusses von IT-Systemen der Leistungserbringer an die TI beauftragt werden, sind gemäß § 332 Abs. 1 SGB V verpflichtet über die notwendige Fachkunde zu verfügen, um Störungen der informationstechnischen Systeme, Komponenten oder Prozesse der Leistungserbringer zu vermeiden. Es ist besondere Sorgfalt bei der Herstellung und Wartung des Anschlusses an die TI walten zu lassen. Die zugrundeliegenden Anforderungen waren im Rahmen zur IT-Sicherheitsrichtlinie[108] in der vertragsärztlichen und vertragszahnärztlichen Versorgung durch die kassenärztlichen Bundesvereinigungen bis zum 30.06.2020 festzulegen. Auch um die Komponenten der TI zu schützen, hat die KBV zusätzlich eine Richtlinie[109] für die Zertifizierung von Dienstleistern gem. § 75b Abs. 5 SGB V beschlossen, um die Arztpraxen in IT-Sicherheitsfragen zu beraten und dabei zu unterstützen, die Vorgaben der IT-Sicherheitsrichtlinie umzusetzen.

8.2 Digitale Verwaltungsleistungen

Durch das Onlinezugangsgesetz (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.

---

[106] Abrufbar unter https://fachportal.gematik.de/anwendungen/
[107] Abrufbar unter https://fachportal.gematik.de/glossar
[108] Abrufbar unter https://www.kvb.de/praxis/it-in-der-praxis/it-sicherheitsrichtlinie/
[109] Abrufbar unter https://www.kbv.de/html/it-sicherheit.php Abrufbar unter https://www.kbv.de/html/it-sicherheit.php

Der GKV-Spitzenverband (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. Urteilsgründe waren, dass es sich bei den sog. Insights-Daten (die untrennbarer Bestandteil einer Fanpage sind und der statistischen Auswertung dienen) aus Sicht des Fanpage-Betreibers zwar um anonyme Daten handelt, aber nicht jeder der gemeinsam Verantwortlichen müsse einen Zugang zu den personenbezogenen Daten haben. Ausschlaggebend sei, dass der Fanpage-Betreiber die Datenverarbeitung veranlasst, indem er eine Fanpage eröffnet und die Nutzenden auf Facebook „lockt“. Er trägt somit maßgeblich zur Datenverarbeitung bei. Der Fanpage-Betreiber habe nachfolgend auch keine Einflussmöglichkeit auf die weitere Datenverarbeitung durch Facebook, aber es reicht aus, dass sich die gemeinsam Verantwortlichen in unterschiedlichen Phasen und Ausmaßen an der Verarbeitung beteiligten. Diese Auffassung des EuGH wurde in einem weiteren Urteil (10.07.2018 – C 25/17) bestätigt.[110]

8.4 Digitale Versorgung — Digitale Gesundheitsanwendungen (DiGA)

8.4.1 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.[111] 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
(siehe Pkt. 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.

[110] https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwioj-Sx_e-AAxVBR_EDHZ-jaAMQQFnoECBMQAQ&url=https%3A%2F%2Fwww.datenschutzkonferenz-online.de%2Fmedia%2Fweitere_dokumente%2FDSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf&usg=AOvVaw39pj_TYf0PCG-xXIxwIaa3&opi=89978449

[111] https://www.bundesamtsozialesicherung.de/de/themen/digitalausschuss/fitness-und-gesundheits-apps-digitale-gesundheits-anwendungen/digitale-gesundheitsanwendungen/

Mit Inkrafttreten des Gesetzes zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz - DVPMG) am 9. Juni 2021 hat der Gesetzgeber dem GKV-Spitzenverband auferlegt, jährlich (erstmals zum 31. Dezember 2021) einen Bericht zu fertigen, wie und in welchem Umfang den Versicherten DiGA nach § 33a Abs. 1 SGB V von den Krankenkassen gewährt werden. Wegen der großen Bedeutung der Schaffung einer neuen Leistungsart ist der vorgesehene Bericht dem Deutschen Bundestag über das Bundesministerium für Gesundheit zu erstatten (§ 33a Abs. 6 SGB V).

DiGA als Satzungsleistung

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 DVPMG 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

Digitale Identitäten im Gesundheitswesen sollen gem. §291 Abs. 8 SGB V ab dem 01.01.2024 als Alternative zu Gesundheitskarten (eGK) eingesetzt werden und bieten Versicherten somit einen kartenlosen Zugang zu allen Anwendungen der Telematikinfrastruktur (TI). Krankenkassen stellen ihren Versicherten auf Wunsch eine digitale Identität in Form einer GesundheitsID zur Verfügung. Die gematik hat durch die Veröffentlichung einer entsprechenden Spezifikation für digitale Identitäten die Grundlage für Krankenkassen geschaffen, um digitale Identitäten zu entwickeln. Die Nutzung bleibt für Anwender:innen freiwillig. Der Zugang zu Online-Gesundheitsanwendungen soll damit erleichtert und über das Smartphone intuitiver werden. Digitale Identitäten ermöglichen es Versicherten, sich künftig über ihr Smartphone in Apps wie das E-Rezept oder die elektronische Patientenakte einzuloggen. Um den Einsatz der digitalen Identität vor Missbrauch zu schützen, ist die gängige 2-Faktor-Authentifizierung vorgesehen. Die Spezifikation sieht vor, dass die GesundheitsID zyklisch durch eine Anmeldung über die Online-Ausweisfunktion des Personalausweises oder über die elektronische Gesundheitskarte (eGK) mit PIN bestätigt werden muss.

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.

8.5 Telemedien

Mit dem Inkrafttreten des TTDSG zum 1. Dezember 2021 traten zeitgleich ein neues Telekommunikationsgesetz (TKG) und Änderungen des TMG in Kraft. Wesentliche Datenschutzvorschriften wurden im TTDSG gebündelt. Es hat u. a. Auswirkungen auf den sehr praxisrelevanten Einsatz von Cookies und ähnlichen Technologien. Auf die Prüfkriterien der Orientierungshilfe für Anbieter von Telemedien der DSK wird verwiesen. [112]

Unabhängig davon, ob ein Personenbezug vorliegt oder nicht, regelt das TTDSG unter anderem den Schutz der Privatsphäre bei der Nutzung von Endeinrichtungen. Das Gesetz enthält besondere Vorschriften zu den technischen und organisatorischen Vorkehrungen, die von Telemedienanbietern zu beachten sind und die Anforderungen an die Erteilung von Auskünften über Bestands- und Nutzungsdaten.

Regelungsbereiche
Die Einwilligungsregelung in § 25 TTDSG ist europarechtskonform und entspricht der Rechtsprechung des BGH zu den Cookie-Einwilligungen. Für Cookies und andere Tracking-Maßnahmen ist auch weiterhin die Einwilligung der Nutzer erforderlich.

Einwilligungsmanagement, § 26 TTDSG
Das Gesetz regelt Dienste zur Verwaltung der erteilten Einwilligungen, sog. „Personal Information Management Services“ (kurz „PIMS“). Nutzer sollen an einer zentralen, neutralen Stelle festlegen können, wie, für welche Zwecke und durch welche Stellen ihre Daten verarbeitet werden dürfen.

Einwilligung der Nutzer
Jeder Zugriff auf und jede Speicherung von Nutzerdaten bedarf auch künftig einer ausdrücklichen, DSGVO-konformen Einwilligung des Endnutzers. Keiner Einwilligung bedürfen nur technisch notwendige Maßnahmen, also solche, die „unbedingt erforderlich“ sind, damit ein vom Nutzer ausdrücklich gewünschter Telemediendienst zur Verfügung gestellt werden kann, § 25 TTDSG. Tracking-Maßnahmen sind neben Cookies zum Beispiel auch das sogenannte Browser-Fingerprinting (Erstellung eines individuellen digitalen Fingerabdrucks), die Nachverfolgung über Werbe-IDs, MAC-Adressen und IMEI-Nummern sowie Smarthome-Anwendungen. Das Gesetz hat folglich einen weiten, technologieneutralen Anwendungsbereich.
Einwilligungen müssen also weiterhin eingeholt werden, beispielsweise mittels Double-Opt-in-Verfahren.

Anwendungsbereich
Betroffen sind alle Anbieter von Telemedien, also aller elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind. Als Anbieter gelten alle natürlichen oder juristischen Personen, die eigene oder fremde Telemedien erbringen, an der Erbringung mitwirken oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermitteln. Neben Online-

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

Angeboten von Waren und Dienstleistungen mit unmittelbarer Bestellmöglichkeit fallen hierunter unter anderem auch Videos-on-Demand (Abrufvideos), Internetsuchmaschinen, Werbe-E-Mails und Homepages zur Information über eine öffentliche Stelle.

Nähere Informationen zur Verbreitung und Einbettung von Videos können dem Schreiben des BfDI vom 14.12.2023 entnommen werden.[113]

[113] siehe Rundschreiben 2024/072 des GKV SV vom 02.02.2024