Leitfaden zur Prüfung von Archivierungs- und Lösch-prozessen

Version 1.2 (27.11.2023)

DIIR-Arbeitskreis Interne Revision in gesetzlichen Kranken- und Pflegeversicherungen

Unterarbeitsgruppe IT-Revision

DIIR Deutsches Institut für Interne Revision e.V.

Vorwort

Grundsätzlich sind personenbezogene Daten (Sozialdaten und Mitarbeiterdaten) unverzüglich zu löschen, soweit sie für die Aufgabenerledigung nicht mehr erforderlich sind. Die Löschung bedarf keines Antrags des Betroffenen, sondern ist von Amts wegen vorzunehmen.

Die Nichtbeachtung von Löschvorgaben ist nach der EU-Datenschutzgrundverordnung mit erheblichen Haftungsrisiken verbunden.

Für einige externe Prüfungen z. B. Prüfung des morbiditätsorientieren Risikostrukturausgleichs (RSA) ist es erforderlich, Dokumentationen bis zum Ende der Prüffristen aufzubewahren. Ansonsten besteht das Risiko, dass nicht vorhandene Daten oder Unterlagen als Fehler gewertet werden.

Daten müssen auch archiviert und gelöscht werden, um den Datenbestand im Hinblick auf Speicherplatz und Systemperformance überschaubar zu halten.

Der Leitfaden soll die Prüfung von Archivierungs- und Löschprozessen unterstützen. Dies gilt sowohl bei Papier als auch für Daten in elektronischer Form.

Inhalt

1 Rechtliche Grundlagen

Gesetz	Details
Sozialgesetzbuch (SGB)	In den folgenden Teilen des Sozialgesetzbuches finden sich Vorgaben zur Aufbewahrung von Daten: SGB I, SGB IV, SGB V, SGB VI, SGB X, SGB XI
EU-Datenschutzgrund-verordnung (DSGVO)	Art. 5 Grundrechte für die Verarbeitung personenbezogener Daten Art. 17 Recht auf Löschung Art. 18 Recht auf Einschränkung der Verarbeitung Art. 25 Technische und organisatorische Maßnahmen
Bundesdatenschutzge-setz (BDSG)	§ 35 Recht auf Löschung
SVRV	§ 14 Aufbewahrung § 17 Einsatz der automatisierten Datenverarbeitung
SRVwV	§ 35 Aufbewahrungsfristen § 36 Aufbewahrung § 40 Sicherheit beim Einsatz der automatisierten Datenverarbeitung i. v. m. Anlage 9 zum § 40
RSAV	§ 7 Verarbeitung von Daten für die Durchführung und Weiterentwicklung des Risikostrukturausgleichs § 15 Zuweisung für Vorsorge- und Früherkennungsmaßnahmen und für strukturierte Behandlungsprogramme
BArchG	Bundesarchivgesetz
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Bü-chern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
AO (Abgabenordnung)	§ 147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen § 147a Vorschriften für die Aufbewahrung von Aufzeichnungen und Unter-lagen bestimmter Steuerpflichtiger

Aus Einzelnormen können sich noch weitere Anforderungen hinsichtlich Aufbewahrungs- und Löschfristen ergeben.

2 Zielfragen

Hier handelt es sich um mögliche übergeordnete Zielfragen, die es im Rahmen der Prüfung zu beantworten gilt.

Zielfragen	**Erläuterungen**
Sind Archivierungs- und Löschprozesse in angemessenen Umfang geregelt?	Dabei ist zu achten, dass sowohl die o. g. rechtlichen Grundlagen als auch die unten angeführten Quellen Berücksichtigung finden.
Werden die Regelungen zu Archivierungs- und Löschprozessen umgesetzt?	Hier geht es darum, inwieweit die geregelten Archivierungs- und Löschprozesse in der Praxis umgesetzt werden.
Sind alle für die Aufgabenerledigung nicht mehr erforderlichen Daten fristgerecht gelöscht?	Diese Frage zielt darauf ab, ob die o. g. Prozesse erfolgreich sind und Daten tatsächlich gelöscht werden.
Werden datenschutzrechtliche Vorgaben eingehalten?	Vor allem geht es um die Einhaltung der Vorgaben aus der DSGVO.
Kann das Risiko von Sanktionen und Bußgeldern in Bezug auf die DSGVO ausgeschlossen werden?	Die Prüfungen der Internen Revision müssen laut Definition u. a. die Effektivität des Risikomanagements bewerten. Das größte Risiko beim Thema Archivierung und Löschung liegt bei Sanktionen und Bußgeldern.

3 Prüfungsfragen

3.1 Aufbauorganisation

Prüfungsfragen Aufbauorganisation	**Erläuterungen**
Ist ein umfassendes Archivierungs- und Löschkonzept vorhanden?	Im Konzept sollten folgende Sachverhalte geregelt sein: ▪ Verantwortung und Zuständigkeiten, technische und organisatorische Anforderungen ▪ Systeme, Informationsbestände, Datenobjekte, Speicherorte und Datenflüsse ▪ Auch Archivsysteme, Testsysteme, Protokolldaten und Backupsysteme ▪ Verfahren zur Datenlöschung, insbesondere Löschregeln mit Löschfrist und Startzeitpunkt ▪ Archivierungs- und Löschfristen; sofern keine rechtlichen Fristen vorliegen, sind eigene Fristen festzulegen ▪ Für elektronische Daten soll bereits zum Archivierungszeitpunkt der Löschzeitpunkt benannt werden ▪ Löschklassen und Standardlöschfristen, Schutzklassen, ▪ Umgang mit unstrukturierten Daten (z. B. Laufwerke) nicht-GKV Standard-Anwendungen ▪ Ausnahmen und Sonderfälle (z. B. Legal Hold; Datensperrung) ▪ Dokumentation der Löschung und Löschprotokoll
Gibt es ein Datenlebenszyklus-Modell?	Wesentliche Fragen sind bereits zu Beginn der Datenentstehung zu klären. ▪ Datenerstellung inkl. Bestimmung eines Dateneigners ▪ Datenspeicherung ▪ Datennutzung ▪ Datenarchivierung ▪ Datenlöschung

Existieren Regelungen zur Datensperrung?	Die Datensperrung sollte in einem speziellen Archiv erfolgen. Dabei sind folgende Grundsätze zu beachten: ▪ Keine Integration in reguläre Verarbeitungsprozesse ▪ Sehr eingeschränkter Personenkreis ▪ Kein Zugriff mit „allgemeinen“ Berechtigungen ▪ Reglementierter Zugriff für besondere Konstellationen
Liegen Regelungen vor, wenn Anwendungen außer Betrieb genommen werden?	Bei Außerbetriebnahme von Anwendungen ist zu klären, inwieweit Daten archiviert, migriert oder gelöscht werden müssen.
Sind die Verantwortlichkeiten und Zuständigkeiten organisatorisch verankert?	Die Verantwortung ist schriftlich zu regeln.
Sind Schnittstellen geklärt?	Schnittstellen sind in einem Schnittstellenkonzept zu regeln.
Existiert eine verbindliche Arbeitsanweisung?	Detaillierte verbindliche Vorgaben zur konkreten Umsetzung des Archivierungs- und Löschkonzepts

3.2 Ablauforganisation

Prüfungsfragen Ablauforganisation	**Erläuterungen**
Existiert ein festgelegter Ablaufprozess?	Mögliche Schritte zum Prozessablauf: ▪ Festlegung von Archivierungs- und Löschfristen ▪ Hinterlegung von Löschfristen im Konzept und in den Systemen ▪ Erstellung Löschauftrag ▪ Genehmigung Löschauftrag ▪ Testlauf und Produktivsetzung der Löschung ▪ Technische und fachliche Überprüfung des Löschlaufs ▪ Dokumentation der Prozessschritte und des Löschergebnisses

Sind Kontrollinstanzen vorhanden, um auszuschließen, dass Daten gelöscht werden, die noch erforderlich sind?	Insbesondere bei externen Prüfungen (z. B. Morbi-RSA) kann es vorkommen, dass Aufbewahrungsfristen verlängert werden müssen.

3.3 Praktische Umsetzung

Prüfungsfragen Praktische Umsetzung	**Erläuterungen**
Werden die Vorgaben im Archivierungs- und Löschkonzept und in der Arbeitsanweisung in der Praxis umgesetzt?	
Finden vor der produktiven Löschung Testläufe statt?	Testläufe sind zu dokumentieren. Fehler aus Testläufen sind zu prüfen und beheben.
Ist der Ablaufprozess nachvollziehbar dokumentiert?	Ziel ist die Nachvollziehung, wann und durch welche Personen oder technische Abläufe die einzelnen Prozessschritte durchgeführt wurden.
Ist das Löschergebnis nachvollziehbar dokumentiert?	Eine vollständige Dokumentation aller gelöschten Daten ist nicht erforderlich und steht im Widerspruch zur Intention der DSGVO. Trotzdem sollten Löschprotokolle mit grundlegenden Informationen zur Löschung vorhanden sein, insbesondere ▪ Dateneigner und Löschverantwortlicher ▪ Zeitpunkt der Löschung ▪ Löschmethode ▪ Löschgegenstand (z. B. Beschreibung und Anzahl Datensätze) ▪ Dokumentation des Löschvorgangs
Sind die Daten tatsächlich gelöscht?	Bestätigung der technischen und fachlichen Überprüfung des Löschlaufs. Ergänzend eigene Überprüfung, ob Daten tatsächlich gelöscht wurden.
Sofern unmittelbar keine Löschung umsetzbar ist, wurden organisatorische und technische Maßnahmen zur Sperrung implementiert?	Dabei ist zu prüfen, ob Zugriffssperren wirksam umgesetzt wurden.

3.4 Datenschutz

Prüfungsfragen Datenschutz	**Erläuterungen**
Existiert ein Verzeichnis der Verarbeitungstätigkeiten?	Das Verzeichnis soll dem Prüfdienst einen Überblick über Verfahren und der damit verbundenen Produkte verschaffen. Löschfristen sind im Verarbeitungsverzeichnis zu definieren.
Liegt eine Verfahrensdokumentation nach Anlage 9 § 40 SRVwV vor?	Die Verfahrensdokumentation soll dem Prüfdienst eine Beschreibung der sachlogischen Lösung der genutzten Produkte verschaffen.
Gibt es eine Aufstellung von Anfragen zur Umsetzung des Betroffenenrechts auf Löschung?	Vgl. Artikel 17 DSGVO
Sind neben den Löschroutinen für Löschungen nach Ablauf der Aufbewahrungsfrist auch Prozesse zur Umsetzung des Betroffenenrechts auf Löschung implementiert?	Vgl. Artikel 17 DSGVO
Sind für Verträge alle erforderlichen Unterlagen vorhanden?	Z. B. Mietverträge, Ausschreibungsunterlagen, Wirtschaftlichkeitsbetrachtungen
Existiert eine Vertragsdatenbank, mit deren Hilfe sämtliche laufenden und abgeschlossenen Verträge mit Auftragsverarbeitung identifiziert werden können?	
Finden sich Regelungen für Auftragsverarbeitung in den Verträgen, die mit dem Archivierungs- und Löschkonzept konform sind?	
Werden Prüfpflichten der Kasse auch bei Dienstleistern wahrgenommen?	Löschnachweise sind insbesondere nach Beendigung des Vertragsverhältnisses einzufordern.

4 Begriffsdefinitionen

Begriffe	Definition
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).
Sozialdaten	Sozialdaten sind personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.
Grunddaten	Als Grunddaten werden Daten bezeichnet, deren Aufzeichnungspflicht unmittelbar aus den gesetzlichen Vorschriften abzuleiten ist.
Belegdaten	Belegdaten sind Daten, die aufgrund gesetzlicher Vorschriften (z. B. SVRV, SRVwV) und der „Grundsätze ordnungsgemäßer Datenverarbeitung“ nachzuweisen sind.
Bearbeitungsdaten	Als Bearbeitungsdaten werden Daten bezeichnet, die für die Sachbearbeitung und für verarbeitungstechnische Vorgänge benötigt werden.
Archivierung	Archivierung im Sinne der Grundsätze ordnungsgemäßer Aufbewahrung ist die logische und physische Trennung bestimmter Daten vom aktuellen Datenbestand mit dem Ziel der langfristigen systematischen Aufbewahrung.
Auslagerung	Auslagerung im Sinne der Grundsätze ordnungsgemäßer Aufbewahrung ist die physische Trennung bestimmter Daten vom aktuellen Datenbestand. Die logische Verknüpfung bleibt dabei erhalten.
Löschung	Daten sind nicht mehr vorhanden bzw. können nicht mehr hergestellt werden.
Legal Hold	In besonderen Situationen kann es erforderlich sein, dass Unterlagen oder Daten zur weiteren Bearbeitung über das Fristende hinaus benötigt werden (z. B. anhängige Gerichtsverfahren, Regressfälle oder Behandlungsfehler). Die Rechtsvorschriften lassen für solche Sondersituationen eine Aussetzung bzw. Verlängerung der Löschfrist zu.
Anonymisierung	Daten werden so verändert, dass sie nicht mehr einer Person zugeordnet werden können.
Pseudonymisierung	Daten werden durch ein Pseudonym ersetzt. Mit Hilfe eines Schlüssels kann der Bezug zu einer Person wiederhergestellt werden.

5 Quellenverzeichnis

Quellenverzeichnis	
Leitfaden elektronische Kommunikation und Digitalisierung in der Sozialversicherung	Leitfaden der Prüfdienste des Bundes und der Länder.
Grundsätze ordnungsgemäßer Aufbewahrung	Grundsätze des GKV-Spitzenverband im Sinne des § 110a SGB IV zur Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen im Bereich der gesetzlichen Kranken- und Pflegeversicherung.
RSA-Prüfhandbücher	Prüfhandbücher und Durchführungshinweise der Prüfdienste des Bundes und der Länder zu RSA-Prüfungen.
Technische Richtlinien BSI	Technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik TR-03125 (TR-ESOR) und TR-03138 (RESISCAN)
Checkliste zur Prüfung der Datenschutzorganisation	Leitfaden des DIIR-Arbeitskreises Datenschutz und Data Governance zur Überprüfung der Datenschutzorganisation und ihrer Wirksamkeit
DIN-Leitlinien	DIN 66398 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten und DIN 66399 Vernichtung von Datenträgern

Autoren

DIIR-Arbeitskreis Interne Revision in gesetzlichen Kranken- und Pflegeversicherungen, Unterarbeitsgruppe IT-Revision

Verfasser des Leitfadens:

- Florian Bloem (AOK RH)
- Jens Brinkmann (KKH)
- Andreas Claus (VIACTIV KK)
- Sandra Gräber (KBS)
- Ralf Heitmann (BIG direkt)
- Kay Henkel (KKH)
- Andreas Holzapfel (AOK Bayern)
- Andreas König (SBK)
- Dirk Lohoff (KBS)
- Sabine Provenzano (Pronova BKK)
- Katja Richter (AOK BaWü)
- Dennis Thöle (hkk Krankenkasse**)**
- Uwe Ulzhöfer (AOK RH)

Rückfragen oder Verbesserungsvorschläge nimmt der Arbeitskreis gerne entgegen.

Veröffentlicht auf www.diir.de

Frankfurt am Main, April 2024

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main