Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autor(en)

Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Gindera, Sarah	CURACON GmbH
Isele, Christoph	Cerner Deutschland GmbH
Koeppe, David	Vivantes - Netzwerk für Gesundheit GmbH
Letter, Michael	5medical management GmbH
Mönter, Johannes	CURACON GmbH
Schlütter, Johannes	net.ter GmbH
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH

Version 1.0

Stand der Bearbeitung: 20. Juni 2020

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
>
> Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
>
> Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Inhaltsverzeichnis

Vorwort

Personenbezogene Daten sollen und dürfen in der Regel nicht auf „Ewigkeiten“ gespeichert werden; wie lange die Speicherung erfolgen soll und darf, muss aber im Einzelfall entschieden werden. Die datenschutzrechtliche Löschpflicht resultiert aus dem Recht der informationellen Selbstbestimmung, aber diese kann nur von lebenden Personen wahrgenommen werden: Das allgemeine aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG resultierende Persönlichkeitsrecht endet mit dem Tod des jeweiligen Menschen.

Gemäß Art. 1 Abs. 2 DS-GVO schützt das europäische Datenschutzrecht die Grundrechte und Grundfreiheiten natürlicher Personen, entsprechend ErwGr. 27 DS-GVO[1] gilt die DS-GVO nicht für Verstorbene, wenngleich die Mitgliedsstaaten speziell für die Verarbeitung von Daten verstorbener Personen Regelungen erlassen dürfen.

Wenngleich der deutsche Gesetzgeber im Rahmen der BDSG-Gesetzgebung von dieser Öffnungsklausel keinen Gebrauch machte, finden sich im bereichsspezifischen Datenschutzrecht Regelungen für den Umgang mit Daten Verstorbener. So beispielsweise:

- § 35 Abs. 5 SGB I (Sozialgeheimnis)
  „Sozialdaten Verstorbener dürfen nach Maßgabe des Zweiten Kapitels des Zehnten Buches verarbeitet werden. Sie dürfen außerdem verarbeitet werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können.“
- § 7 Abs. 1 S. 3 Hamburgisches Krankenhausgesetz (HmbKHG)
  „Der Datenschutz endet nicht mit dem Tode der Patientin oder des Patienten.“

Die datenschutzrechtlich gebotene Löschung kann also nicht mit Verweis auf den Tod eines Patienten negiert werden. Vielmehr muss überprüft werden, ob bereichsspezifische Regelungen trotz des Versterbens eines Patienten eine Löschung fordern[2].

In diesem Sinne ist es unumgänglich für jeden Verantwortlichen, sich mit dem Thema „löschen“ auseinanderzusetzen und Regelungen zu erlassen, wie in seinem Verantwortungsbereich mit diesem Thema umgegangen wird. Dazu dient ein Löschkonzept.

Diese Praxishilfe ist in verschiedene Teile gegliedert:

- Teil I beinhaltet allgemeine Informationen bzgl. der gesetzlichen Rahmenbedingungen, welchen genügt werden muss.
- Teil II beschreibt den Aufbau und die Struktur eines Löschkonzeptes
- Teil III enthält Beispiele, welche als Anregungen zur Umsetzung der in Teil I und Teil II beschriebenen Hinweise dienen.

[1] ErwGr. 27: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.“

[2] Gutachten der Datenethikkommission der Bundesregierung, S. 111: „Da **der Schutz durch die DSGVO mit dem Tod erlischt**, stehen sodann, nach derzeitiger Gesetzeslage, auch keine datenschutz-rechtlichen Eingriffsmöglichkeiten zur Verfügung, die Angehörige geltend machen könnten. Dass damit die personenbezogenen Daten Verstorbener in die nahezu unbegrenzte Verfügungsgewalt der jeweiligen Verantwortlichen übergehen, erscheint ethisch bedenklich. Die DEK empfiehlt der Bundesregierung daher, nach dem Vorbild mehrerer europäischer Staaten von der in Erwägungsgrund 27 zur DSGVO erwähnten Möglichkeit Gebrauch zu machen, Regelungen zum **postmortalen Datenschutz** zu erlassen. Dabei sollten Angehörige fundamentale Betroffenenrechte – etwa auf Löschung von Daten oder Korrektur unrichtiger Daten – auch nach dem Tod des Betroffenen geltend machen können.“ [Online] 2019 [Zitiert 2020-05-23] Verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

Teil I: Löschkonzept: Was ist aus gesetzlicher Sicht zu beachten?

1 Einleitung

Tätigkeiten ohne die Verarbeitung personenbezogener Daten (pbD) sind in der Gesundheitsversorgung nur in den seltensten Fällen möglich. Eine Patientenversorgung ohne die Verarbeitung von Patientendaten ist nicht möglich, auch die medizinische Forschung ist ohne Daten – seien es Patienten- oder Probandendaten - nicht durchführbar. Selbst im Bereich der Medizingeschichte ist vieles mit Personennennungen verbunden, wenngleich in diesen Fällen sehr häufig auch mit Daten verstorbener Personen gearbeitet wird.

Personenbezogene Daten, welche erhoben und genutzt werden, müssen auch wieder gelöscht werden. Diese Vorgabe existierte schon in den „alten" deutschen Datenschutzregelungen, bevor es die Datenschutz-Grundverordnung (DS-GVO) gab, aber diese gesetzliche Pflicht findet sich natürlich auch in der DS-GVO wieder. Im Rahmen der zur Verfügung zu stellenden Informationen gem. Artt. 13 Abs. 2 lit. a und 14 Abs. 2, lit. a DS-GVO muss die Speicherdauer personenbezogener Daten angegeben werden oder, wenn dieses nicht möglich ist, sind Kriterien für die Festlegung der Speicherdauer zu benennen. Somit ist, um die Speicherdauer zu begrenzen, eine Löschung vorzusehen. Unabhängig hiervon richtet der aus Art. 5 Abs. 1 lit. e DS-GVO resultierende Grundsatz der Speicherbegrenzung an den Verantwortlichen bei jeder Verarbeitung personenbezogener Daten die Forderung, den Zeitraum der Identifizierbarkeit betroffener Personen auf den zur Erfüllung der oder des Verarbeitungszwecke(s) erforderlichen Zeitraum zu beschränken, wenn nicht gesetzliche Vorgaben anderes bestimmen. Diese Anforderung kann nur erfüllt werden, wenn die Dauer der Identifizierbarkeit begrenzt wird, d. h. die identifizierenden Daten müssen gelöscht werden. Dies kann in der betrieblichen Praxis nur durch ein Löschkonzept nachweislich gewährleistet werden[3].

Verantwortliche müssen Daten löschen und dies auch von Anfang an einplanen; diese erforderliche Planung der Löschung der Daten schon vor deren Erhebung, also vor dem eigentlichen Verarbeitungsbeginn, resultiert z. B. aus den Vorgaben von Art. 25 DS-GVO: Der Verantwortliche *trifft sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung* geeignete technische und organisatorische Maßnahmen, *um die Datenschutzgrundsätze wie etwa Speicherbegrenzung* wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen.

Die Planung der Löschung der personenbezogenen Daten beinhaltet den gesamten Prozess des Löschens, dies beinhaltet z. B.:

- Ermittlung aller durch das Unternehmen verarbeiteten personenbezogenen Daten,

[3] Auch das Bundesministerium für Wirtschaft und Energie (BMWi) empfiehlt ein Löschkonzept als „Best Practice": „Um den Löschpflichten der DSGVO gerecht zu werden, sollten die Unternehmen sogenannte Löschkonzepte (z. B. nach DIN 66398) entwickeln, welche es ermöglichen, in regelmäßigen Abständen Löschungen durchzuführen." Quelle: BMWi „Orientierungshilfe zum Gesundheitsdatenschutz", Seite 38 Kapitel. [Online] 2018 [Zitiert 2020-04-23] Verfügbar unter https://www.bmwi.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=16

- Festlegung, welche Daten wann unter welchen Umständen von wem wie gelöscht werden,
- wie der Nachweis der Löschung geführt wird,
- Feststellung, für welche Daten welche gesetzlichen Aufbewahrungsvorschriften existieren und die somit während dieser Zeitspanne nicht gelöscht werden dürfen.

Diese Prozessbeschreibung wird i. d. R. in einem „Löschkonzept" festgehalten. Dieses Löschkonzept dient zugleich als Nachweis gegenüber betroffenen Personen sowie Datenschutz-Aufsichtsbehörden, dass das Thema der Datenlöschung vom Verantwortlichen adressiert, geplant und in die betriebliche Organisation integriert wurde.

Die Art des Löschens bleibt dabei dem oder den jeweiligen Verantwortlichen überlassen: ob eine physikalische Vernichtung, eine Anonymisierung oder irgendetwas anderes gewählt wird, liegt allein in der Entscheidungshoheit des Verantwortlichen – die gesetzlichen Rahmenbedingungen sind technikneutral[4]. Entsprechend Art. 5 Abs. 1 lit. e DS-GVO muss eine Löschung sicher gewährleisten, dass die Identifizierung der betroffenen Personen nicht mehr möglich ist und dies muss der Verantwortliche auch nachweisen können. Dementsprechend urteilte die österreichische Aufsichtsbehörde völlig zu Recht im Jahre 2018 [5]: „Die Entfernung des Personenbezugs („Anonymisierung") von personenbezogenen Daten kann somit grundsätzlich ein mögliches Mittel zur Löschung i.S.v. Art. 4 Z 2 i.V.m. Art. 17 Abs. 1 DS-GVO sein. Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann."

Ein wesentliches Problem für die Ermittlung des Löschbedarfs ist, dass personenbezogene Daten in unterschiedlichsten Systemen und Formaten vorliegen können und womöglich auch redundant vorhanden sind. Personenbezogene Daten können einerseits in Form von (mehr oder weniger) strukturierten Datensätzen in einer Datenbank enthalten sein, wie beispielsweise einem Krankenhaus-Informationssystem (KIS) oder einem Labor-Informationssystem (LIS). Daneben werden im Gesundheitsbereich Daten aber auch in Datenbeständen, deren Struktur die Benutzer im Wesentlichen selbst beeinflussen können, wie beispielsweise Verzeichnisse auf Laufwerken, in denen Dateien mit Texten, Tabellen, Präsentationen, Fotos oder Videos gespeichert werden, verarbeitet. Das Löschkonzept des Verantwortlichen muss grundsätzlich alle personenbezogenen Daten umfassen [6], sowohl die in Datenbanken als auch in Dateisystemen/Ordnern gespeicherten personenbezogenen Daten. Dabei stellt die Speicherung personenbezogener Daten in Dateisystemen/Ordnern Verantwortliche vor besondere Herausforderungen: Die Verantwortlichen wissen ggf. nicht, was wo von wem gespeichert wurde. D. h. um hier seinen gesetzlichen Verpflichtungen genügen zu können, muss der Verantwortliche sein Weisungsrecht (sei es aus dem Arbeits- oder Vertragsrecht resultierend) nutzen und Weisungen erlassen, wie mit diesen unstrukturiert gespeicherten Daten umzugehen ist.

[4] ErwGr. 15 S. 1 DS-GVO: „Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen,"

[5] Österreichische Datenschutzbehörde: Bescheid v. 5.12.2018, Gz. D123.270/0009-DSB/2018. [Online] 2018 [Zitiert 2020-03-24] Verfügbar unter https://www.ris.bka.gv.at/, Geschäftszahl DSB-D123.270/0009-DSB/2018

[6] Laut Art. 2 Abs. 1 DS-GVO fallen personenbezogene Daten, die automatisiert, teilweise automatisiert oder auch nicht-automatisiert verarbeitet werden, unter die Regelungen der DS-GVO, nicht-automatisiert verarbeitete Daten jedoch nur, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Weiterhin regeln einige Spezialgesetze den Umgang mit „Patientendaten". Einige dieser Gesetze geben auch eine Begriffsbestimmung zu „Patientendaten", jedoch wird hierbei nicht zwischen automatisierter und nicht-automatisierter Verarbeitung unterschieden. Daher empfiehlt es sich, das Löschkonzept für alle personenbezogenen Daten anzuwenden.

2 Gesetzliche Rahmenbedingungen

Um das Thema „Löschen“ datenschutzrechtlich betrachten zu können, müssen verschiedene Aspekte betrachtet werden:

1) Was ist unter dem Begriff „Löschen“ zu verstehen?
2) Wer muss löschen?
3) Wann darf gelöscht werden?
4) Wann muss man löschen?
5) Wie muss man löschen?
6) Welche Konsequenzen drohen, wenn man nicht löscht?
7) „Nebenpflichten“ einer Löschung
8) Wunsch der Datenaufbewahrung vs. Löschpflichten
9) Gesetzliche Aufbewahrungspflichten

2.1 Was ist unter dem Begriff „Löschen“ zu verstehen?

Seit die DS-GVO in Wirkung getreten ist, ist diese in Europa gegenüber nationalem Recht vorrangig anzuwenden. Demnach stellt die Löschung eine Form der Verarbeitung i. S. d. Art. 4 Ziff. 2 DS-GVO dar[7], wobei „Löschung“ selbst durch die DS-GVO allerdings nicht näher definiert wird.

Entsprechend dem Urteil des Europäischen Gerichtshofs vom 13. Mai 2014[8] ist der Begriff „Löschen“ im Sinne von „Löschen im physikalischen Sinn“ oder als irreversible Anonymisierung anzusehen. In gleicher Weise äußert sich die Artikel-29-Gruppe in ihrer Stellungnahme[9] zu Datenschutzfragen im Zusammenhang mit Suchmaschinen. Eine Anonymisierung muss jedoch vollständig unumkehrbar sein, damit die Datenschutzbestimmungen nicht länger gelten und dem Begriff des „Löschens“ entsprochen wird.

Diese Auffassung wird auch in anderen Ländern Europas geteilt. Der Oberste Gerichtshof, die oberste Instanz in Zivil- und Strafsachen in Österreich, versteht unter Löschen einen Vorgang, der zu einem unwiderruflichen Beseitigen der Daten führt[10]. Darunter versteht der ÖOGH Maßnahmen, welche bewirken, dass die Daten nicht mehr verfügbar sind.

2.2 Wer muss löschen?

Entsprechend den gesetzlichen Vorgaben ist zum Löschen der für die Verarbeitung personenbezogener Daten Verantwortliche i. S. d. Art. 4 Ziff. 7 DS-GVO verpflichtet. Dies ist in der Regel die Unternehmensleitung, also z. B. der Inhaber einer Arztpraxis.

Auftragsverarbeiter dürfen grundsätzlich nur auf Weisung eines Verantwortlichen löschen. Daher sieht Art. 28 Abs. 3 S. 2 lit. g DS-GVO vor, dass nach Abschluss der Erbringung der Verarbeitungsleistungen, also unmittelbar vor zeitlicher Beendigung der Dienstleistungstätigkeit und

[7] Dix A.:. Art. 17 Rn. 5. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[8] EuGH, Urteil vom 13. 5. 2014 - C-131/12. [Online] 2014 [Zitiert 2020-03-24] Verfügbar unter https://dejure.org/2014,9457

[9] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen. [Online] 2008 [Zitiert 2020-03-24] Verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_de.pdf

[10] ÖOGH AZ 6 Ob 41/10p, Urteil vom 15.4.2010 [Online] 2008 [Zitiert 2020-03-24] Verfügbar unter http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20100415_OGH0002_0060OB00041_10P0000_000

vor Ende des Vertragsverhältnisses, der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder an diesen zurückgibt und alle beim Auftragsverarbeiter evtl. vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

2.3 Löschpflicht

Einerseits sieht Art. 5 Abs. 1 lit. d DS-GVO eine Löschpflicht beim Vorliegen unrichtiger Daten vor, andererseits enthält Art. 17 Abs. 1 DS-GVO Verpflichtungen auch für andere Fälle. Im Gegensatz zu anderen Betroffenenrechten enthält Art. 17 Abs. 1 DS-GVO auch Pflichten, welchen der Verantwortliche unterliegt und die eine Löschpflicht beinhalten, ohne dass die betroffene Person agieren muss[11]. Entsprechend den rechtlichen Vorgaben sind personenbezogene Daten unverzüglich zu löschen, wenn einer der im Folgenden aufgeführten Tatbestände zutrifft:

a) Die betroffene Person die Löschung verlangt und keine rechtlichen Gründe die weitere Verarbeitung und insbesondere die Speicherung erlauben.
b) Die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.
c) Die betroffene Person ihre Einwilligung zur Verarbeitung widerruft und eine anderweitige Rechtsgrundlage für die Verarbeitung/Speicherung wie z. B. gesetzliche Aufbewahrungspflichten fehlt.
d) Die betroffene Person gemäß Art. 21 Abs. 1 Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen.
e) Die betroffene Person gemäß Art. 21 Abs. 2 Widerspruch gegen die Verarbeitung zu Zwecken der Direktwerbung einlegt
f) Die personenbezogenen Daten unrechtmäßig verarbeitet wurden/werden. Damit ergibt sich insbesondere, dass unzulässig erhobene personenbezogene Daten umgehend gelöscht werden müssen, desgleichen falsche Daten, sofern hier keine gesetzlichen Erfordernisse eine Löschung verbieten. Grundsätzlich besteht nach Art. 17 Abs. 1 lit. d DS-GVO eine Löschpflicht, wenn die Zulässigkeit der Verarbeitung nicht den Anforderungen der DS-GVO genügt.
g) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, welcher der Verantwortliche unterliegt, erforderlich; dies schließt neben Gesetzen der EU und Mitgliedstaaten auch Verpflichtungen ein, welche aus Gerichtsurteilen resultieren sowie Anordnungen entsprechend Art. 58 Abs. 2 DS-GVO einer Datenschutz-Aufsichtsbehörde. Allerdings muss es sich um eine Rechtspflicht des objektiven Rechts handeln, demzufolge eine vertraglich gegenüber einem Dritten eingegangene Pflicht alleine nicht ausreicht; Löschen stellt eine Verarbeitung dar und der Verantwortliche kann sich durch einen Vertrag mit einem Dritten keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten verschaffen[12].

[11] So z. B.:
- Herbst T.: Art. 17 Rn. 8. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5
- Dix A.: Art. 17 Rn. 6. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[12] Herbst T.: Art. 17 Rn. 29. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

h) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 erhoben.

Zu beachten: In einigen Fällen sieht der europäische Gesetzgeber ein Wahlrecht hinsichtlich des Tatbestandes „Löschen personenbezogener Daten" seitens der betroffenen Person vor:

- Sind die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig (Art. 17 Abs. 1 lit. a DS-GVO), so kann es dennoch sein, dass die betroffene Person diese Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt; in diesen Fällen kann die betroffene Person verlangen, dass die Daten in ihrer Verarbeitung eingeschränkt und nicht gelöscht werden.
- In Fällen einer unrechtmäßigen Verarbeitung (Art. 17 Abs. 1 lit. d DS-GVO) hat die betroffene Person entsprechend Art. 18 Abs. 1 lit. b DS-GVO ein Wahlrecht, ob die Daten gelöscht werden oder ob die Verarbeitung eingeschränkt wird.

In beiden Fällen muss daher vor der Löschung eine Prüfung erfolgen, ob die betroffene Person kontaktiert und deren Entscheidung abgewartet werden muss; in diesen Fällen sind die Daten bis zu dieser Entscheidung zu sperren[13, 14].

2.3.1 Löschung vs. gesetzliche Aufbewahrungspflicht

Die gesetzlichen Aufbewahrungsfristen *verlangen* eine Aufbewahrung von Patientendaten, dementsprechend darf während dieses gesetzlich vorgeschriebenen Zeitraums keine Löschung erfolgen.

Eine Arztpraxis oder ein Krankenhaus muss die Dokumentation der Krankenbehandlung aufbewahren. Entsprechend § 630f BGB[15] gilt:

> *Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen.*

Dementsprechend dürfen auch unrichtige Einträge während der Zeitdauer der gesetzlichen Aufbewahrungsvorgaben nicht gelöscht werden, vielmehr muss hier eine Sperrung veranlasst werden.

2.3.2 Erlaubnistatbestand zur Speicherung: „Schutz vor Schadensersatzansprüchen"?

Entsprechend § 197 Abs. 1 Ziff. 1 BGB [16] existiert eine dreißigjährige Verjährungsfrist bzgl. „Schadensersatzansprüche, die auf der vorsätzlichen Verletzung des Lebens, des Körpers, der Gesundheit, der Freiheit oder der sexuellen Selbstbestimmung beruhen". Ein legitimer Verwendungszweck der Daten der Gesundheitsversorgung seitens des Leistungserbringers ist es, sich gegen unrechtmäßige Schadensersatzansprüche wehren zu können.

[13] Dix A.: Art. 17 Rn. 6. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[14] Herbst T.: Art. 17 Rn. 10, 14. In: Kühling/Buchner (Hrsg.) DS-GVO BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

[15] Bürgerliches Gesetzbuch (BGB) § 630f Dokumentation der Behandlung. [Online] 2013 [Zitiert 2020-03-24] Verfügbar unter http://www.gesetze-im-internet.de/bgb/__630f.html

[16] Bürgerliches Gesetzbuch (BGB). § 197 Dreißigjährige Verjährungsfrist. [Online] 2013 [Zitiert 2020-03-24] Verfügbar unter http://www.gesetze-im-internet.de/bgb/__197.html

Daher ist eine 30jährige Aufbewahrung erlaubt, wenn hinreichender Tatbestand auf einen Rechtsstreit besteht[17]. „Hinreichender Tatbestand" ist ein unbestimmter Rechtsbegriff. Analog zu den Regelungen der StPO kann dies für den vorliegenden Sachverhalt dahingehend interpretiert werden, dass ein hinreichender Tatverdacht angenommen werden kann, wenn nach vorläufiger Bewertung des gesamten bekannten Sachverhalts eine Klage bzgl. Schadensersatz für den individuellen Fall angenommen werden kann.

Der Verantwortliche muss hierbei den hinreichenden Tatbestand für den individuellen Fall nachweisen. D. h. eine Löschung kann an Hand dieser Begründung nur unterbleiben, wenn ein konkreter Rechtsstreit ansteht oder mit hinreichender Wahrscheinlichkeit ein entsprechender Rechtsstreit zu erwarten ist; eine grundsätzliche Aufbewahrung aller personenbezogener Daten mit dieser Begründung ist regelhaft nicht statthaft[18]. Seitens des Verantwortlichen ist daher eine Risikoabwägung erforderlich: „Wie wahrscheinlich ist ein Rechtsstreit?" Dies kann beispielsweise durch eine Untersuchung, wie oft bei bestimmten medizinischen Eingriffen ein Rechtsstreit nach Ablauf der gesetzlichen Aufbewahrungsfrist erfolgte, ermittelt werden. Hierzu können beispielsweise Daten aus den Rechtsstreitigkeiten der letzten 5 Jahre genutzt werden und das Ergebnis in die Risikoabwägung einfließen. Das Ergebnis könnte z. B. wie folgt aussehen:

- Bypass-OP Kardiochirurgie: 5% Streitigkeiten nach Ablauf der 10jährigen gesetzlichen Aufbewahrungsfrist
  → Akten werden entsprechend der Frist, in welcher ein Rechtsstreit wahrscheinlich ist, aufbewahrt
- Enukleation: 0% Rechtsstreit nach Ablauf der 10-Jahres-Frist
  → sofortiges Löschen.

Die Risikogrenze wird hierbei vom Verantwortlichen festgelegt, aber die Höhe des Risikos, das man tragen will, muss zum Gesamtbild passen. Oder anders ausgedrückt: Andere Risiken, die man durch eine weitere Speicherung eingeht, müssen berücksichtigt werden. Ein Beispiel für andere Risiken ist:

- Welches Risiko bzgl. IT-Sicherheitsvorfällen ist man bereit einzugehen? Hinweise darauf, wie hoch oder niedrig das akzeptable Risiko angesehen wird, sind in diesem Fall Informationen wie beispielsweise
  - Gut geschultes Personal für Firewall, Virenschutz usw. vorhanden?
  - Werden regelmäßig Penetrationstests durchgeführt.
  - Erfolgt ein jährliches externes Audit?
  - Existiert eine Zertifizierung?

[17] So z. B.:
- Kühling J, Klar M. (2014) Löschpflichten vs. Datenaufbewahrung Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten. ZD 10: 506-510
- Herbst T.: Art. 17 Rn. 19. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

[18] Im Patientenrechtegesetz wurde bzgl. zivilrechtlicher Haftung auf „Einzelfälle" verwiesen: „Soweit es […] die Gegebenheiten **im Einzelfall** jedoch erfordern, kann die Aufbewahrungsfrist des Absatzes 3 allerdings auch weit über zehn Jahre hinausgehen. Dies kann insbesondere unter Berücksichtigung der Verjährung von zivilrechtlichen Ansprüchen des Patienten gelten, die nach der Höchstverjährungsfrist des § 199 Absatz 2 erst nach 30 Jahren verjähren können."
Siehe Bundesregierung, BT-Drs. 17/10488: Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten. Seite 26, 2. Spalte 3. Absatz. [Online] 2013 [Zitiert 2020-04-10] http://dipbt.bundestag.de/dip21/btd/17/104/1710488.pdf

Entfällt die Möglichkeit einer entsprechenden Klage (z. B. durch Tod des Patienten, keine Erben vorhanden), müssen die Daten nach Ablauf der Aufbewahrungsfrist und nach Eintreten des Ereignisses, welche eine Klage unmöglich macht, gelöscht werden.

2.3.3 Einschränkung der Löschpflicht

Die gesetzliche Verpflichtung zum Löschen wird in Art. 17 Abs. 3 DS-GVO aber auch eingeschränkt. Dementsprechend gilt das in Art. 17 DS-GVO verankerte Betroffenenrecht auf Löschung der eigenen Daten in den folgenden Fällen nicht:

- Die Verarbeitung der personenbezogenen Daten ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich; in diesen Fällen ist eine Einzelfallbetrachtung erforderlich, ob im jeweiligen Fall das Recht auf freie Meinungsäußerung und Information das Recht auf Löschung überwiegt.
- Wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche nach dem Recht der Union oder der Mitgliedstaaten unterliegt, erforderlich ist, ist das Recht auf Löschung der betroffenen Person ebenfalls eingeschränkt.
- Werden die personenbezogenen Daten zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, verarbeitet, so ist das Recht auf Löschung der betroffenen Person hierdurch eingeschränkt.
- Ist die Verarbeitung der personenbezogenen Daten zur Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt, welche dem Verantwortlichen übertragen wurde, erforderlich, so wird das Recht auf Löschung der betroffenen Person ebenfalls eingeschränkt.
- Ist die Verarbeitung personenbezogener Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gem. Art. 9 Abs. 2 lit. h, i DS-GVO erforderlich und ist Art. 9 Abs. 3 DS-GVO gewährleistet, so wird das Recht auf Löschung der betroffenen Person hierdurch beschränkt.
- Ist die Verarbeitung personenbezogene Daten für
  - im öffentlichen Interesse liegende Archivzwecke,
  - wissenschaftliche oder historische Forschungszwecke

  oder
  - für statistische Zwecke

  gemäß Art. 89 Abs. 1 DS-GVO erforderlich, wird das Recht auf Löschung eingeschränkt, soweit dies voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt; entsprechend Art. 5 Abs. 2 DS-GVO muss dies natürlich nachgewiesen werden können.
- Ist die Verarbeitung personenbezogene Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich, so ist für diesen Zeitraum das Recht auf Löschung nicht anzuwenden.

2.4 Wann muss gelöscht werden?

Der Verantwortliche muss bei Vorliegen einer Löschpflicht die zur Löschung (oder ggf. auch Einschränkung der Verarbeitung) erforderlichen Maßnahmen unverzüglich treffen. Wird die Löschung von einer betroffenen Person verlangt, steht dem Verantwortlichen jedoch eine angemessene Frist zur Prüfung zu, ob eine Löschpflicht besteht; in der Literatur gibt es Meinungen,

dass die in Art. 12 Abs. 3 S. 1 DS-GVO angegebenen Monatsfrist nicht verlängert werden darf[19]. Andere Autoren sehen diese Einschränkung hingegen nicht und sehen eine Verlängerung entsprechend Art. 12 Abs. 2 S. 2 DS-GVO als möglich an[20].

2.5 Wann darf gelöscht werden?

Grundsätzlich steht es einem Verantwortlichen frei, bei ihm bzw. in seinem Auftrag gespeicherte personenbezogene Daten jederzeit zu löschen. D. h. eine Löschung personenbezogener Daten ist jederzeit zulässig.

Eine Löschung ist nur dann unzulässig, wenn der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen oder wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Unter der Berücksichtigung, dass die schutzwürdigen Interessen eines Betroffenen beachtet werden müssen, ist eine Löschung auch dann unzulässig, wenn sie zur Unvollständigkeit oder sonstigen Unrichtigkeit der zulässigerweise gespeicherten verbleibenden Daten führen würde.

2.6 Sonderfall: Einsatz mehrerer Informationssysteme

In einem Krankenhaus werden Daten in mehreren Systemen getrennt gespeichert: Radiologie-Informationssystem, Labor-Informationssystem, Kardiologisches Informationssystem, Onkologisches-Informationssystem usw. Zur Wahrung der schutzwürdigen Interessen eines Betroffenen darf kein System Daten löschen - es sei denn, eine Rechtsvorschrift erlaubt oder ordnet eine Löschung an -, die von einem anderen System benötigt werden, um damit die Vollständigkeit bzw. die Richtigkeit der in diesem System erfolgten medizinische Dokumentation zu gewährleisten.

Soll in einem elektronischen Informationssystem daher eine Löschung von Daten durchgeführt werden, muss zunächst überprüft werden, ob die zu löschenden Daten von einem anderen System zur Gewährleistung der Betroffenenrechte in diesem System benötigt werden. Werden die Daten in einem anderen System benötigt, muss eine Löschung der Daten unterbleiben.

Anderseits werden Daten auch redundant gespeichert. Beispielsweise wird die Bestimmung der Blutgruppe sowohl im Informationssystem des Labors als auch in der Patientenakte, also im KIS, gespeichert. Obwohl es sich um dasselbe Datum handelt, können hier unterschiedliche Vorgaben existieren, sodass ggf. im Labor-Informationssystem das Datum schon gelöscht werden muss, obgleich es im KIS im Rahmen der Vorgaben für die Patientenakte noch weiterhin aufbewahrt werden muss.

2.7 Wie muss man löschen?

Eine **irreversible** Vernichtung der identifizierenden Daten stellt die Löschung dar. Insbesondere stellt Anonymisierung weiterhin eine Form des Löschens dar[21]. Dabei liegt entsprechend Art. 5 Abs. 2 DS-

[19] So z. B.
- Dix A.: Art. 17 Rn. 8. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7
- Dix A.: Art. 12 Rn. 26. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[20] Herbst T.: Art. 17 Rn. 46. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

[21] Entscheidung der Datenschutzbehörde Österreich vom 5.12.2018, Geschäftszahl DSB-D123.270/0009-DSB/2018. [Online] 2018 [Zitiert 2020-03-24] Verfügbar unter

GVO die Nachweispflicht bzgl. der Löschung beim Verantwortlichen, d. h. der Verantwortliche muss die irreversible Vernichtung der Personenbeziehbarkeit bzw. auch das Vorliegen anonymer Daten nachweisen. Grundsätzlich findet man in der Literatur[22] zwei Möglichkeiten:

1. Physikalische Lösung und
2. logische Löschung.

2.7.1 Physikalisches Löschen

Unter physikalischer Löschung wird einerseits die ordnungsgemäße Vernichtung des betreffenden Datenträgers verstanden.

Ebenfalls zur physikalischen Löschung wird die Vernichtung der Daten durch (mehrfaches) Überschreiben verstanden. Der Erfolg einer Löschhandlung tritt erst dann ein, wenn Daten tatsächlich überschrieben werden[23] und auch mit entsprechenden recovery-Tools nicht mehr wiederherstellbar sind.

2.7.2 Logisches Löschen

Die Löschung einer Verknüpfung, eines Verweises im Dateisystem oder einer „Sicht" auf personenbezogene Daten bzw. den entsprechenden Datensatz wird als logische Löschung bezeichnet. Eine logische Löschung führt in aller Regel nicht zu einer tatsächlichen Löschung[24]; die personenbezogenen Daten sind nicht gelöscht, sondern bestenfalls schwieriger auffindbar. Bei der Beurteilung, ob eine Löschung erfolgte oder nicht, müssen insbesondere die Möglichkeiten der Wiederherstellung durch entsprechende Spezialprogramme wie forensische IT-Werkzeuge oder Datenrettungs-Tools berücksichtigt werden.

2.8 Welche Konsequenzen drohen, wenn man nicht löscht?

2.8.1 Möglichkeiten der betroffenen Person

Wird eine Löschung vom Verantwortlichen verweigert oder nicht entsprechend den Vorgaben der DS-GVO durchgeführt, kann sich eine betroffene Person nach Art. 77 DS-GVO bei der zuständigen Aufsichtsbehörde beschweren, auch kann die betroffene Person einen Rechtsbehelf nach Art. 79 DS-GVO einlegen; Letzteres führt zwingend zu einer gerichtlichen Überprüfung des Verhaltens des Verantwortlichen.

2.8.2 Bußgeld

Das Unterlassen einer erforderlichen Löschung stellt eine unrechtmäßige Verarbeitung und damit sowohl einen Verstoß gegen die in Art. 5 DS-GVO beschriebenen Grundsätze für die Verarbeitung als auch einen Verstoß gegen Artt. 6, 7 DS-GVO dar. Dies ist eine Ordnungswidrigkeit und entsprechend Art. 83 Abs. 5 lit. a DS-GVO können bei diesen Verstößen Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Vorjahresumsatzes verhängt werden, je nachdem, welcher der Beträge höher ist.

---

https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

[22] Z. B. Dix A.: Art. 17 Rn. 5. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

[23] Herbst T.: Art. 17 Rn. 38. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

[24] Dix A.: Art. 17 Rn. 5. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

Gleiches gilt, wenn das Betroffenenrecht auf Löschung nicht umgesetzt wird. Gemäß Art. 83 Abs. 5 lit. b DS-GVO werden auch bei derartigen Verstößen die oben beschriebenen Geldbußen verhängt.

2.8.3 Abhilfebefugnisse der Datenschutz-Aufsichtsbehörde

Ein Verstoß gegen die Löschpflichten kann auch dazu führen, dass eine zuständige Aufsichtsbehörde die in Art. 58 DS-GVO beschriebenen Abhilfebefugnisse anwenden kann.

Insbesondere kann eine Datenschutz-Aufsichtsbehörde entsprechend Art. 58 Abs. 2 lit. d DS-GVO einen Verantwortlichen oder Auftragsverarbeiter anweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen. D. h. die Aufsichtsbehörden können vorgeben, *wie* eine Verarbeitung geändert werden muss, damit sie den Anforderungen der DS-GVO genügt.

Ebenfalls zu den Abhilfebefugnissen gehört die in Art. 58 Abs. 2 lit. f DS-GVO beschriebene Möglichkeit, dass Aufsichtsbehörden eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen.

2.8.4 Straftat

Entsprechend § 42 Abs. 2 Ziff. 1 BDSG kann mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden, wer personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet, ohne hierzu berechtigt zu sein. Wird ein erforderliches Löschen nicht durchgeführt, so fehlt der weiteren Speicherung die Rechtsgrundlage, sodass die Speicherung eine unberechtigte Verarbeitung im Sinne von § 42 Abs. 2 Ziff. 1 BDSG darstellen kann.

2.9 „Nebenpflichten“ einer Löschung

Machten Verantwortlicher Daten „öffentlich“, z. B. durch Weitergabe[25] an Dritte, so resultiert bei Vorliegen einer Löschpflicht entsprechend Art. 17 Abs. 2 DS-GVO die Pflicht, „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art,“ zu treffen, um (andere) Verantwortliche bzgl. der Löschpflicht hinsichtlich der bei ihnen gespeicherten Kopien, Replikationen usw. zu informieren. Natürlich müssen die informierten Verantwortlichen selbst entscheiden, ob aufgrund der für sie geltenden Rahmenbedingungen die Löschpflicht auch für sie gilt oder ob auf Grund gesetzlicher Vorgaben eine weitere Speicherung notwendig ist.

Gemäß Art. 19 DS-GVO müssen Verantwortliche allen Empfängern die Löschung ebenfalls mitteilen, außer, dies ist unmöglich oder mit einem unverhältnismäßigen Aufwand[26] verbunden.

2.10 Gesetzliche Aufbewahrungspflichten

Der deutsche (wie grundsätzlich auch der europäische) Gesetzgeber kann gesetzlich festlegen, dass bestimmte Daten von Verantwortlichen für einen festgelegten Zeitraum aufbewahrt und bei Bedarf zu fest definierten Zwecken, wie beispielsweise einer Prüfung durch die Datenschutz-Aufsichtsbehörden oder innerhalb eines Gerichtsprozesses vorgelegt werden müssen. Diese gesetzlichen zeitlichen Vorgaben werden „Aufbewahrungsfristen“ genannt.

[25] Eine Weitergabe im Sinne der Übermittlung an einen Dritten ist hier nicht gemeint, Veröffentlichung beinhaltet eine Weitergabe an mehrere Dritte.

[26] Hinweis: Das Provinzgericht Warschau schreibt in seinem Urteil, dass die durch Information per Telefon oder Post entstehenden Kosten keinen unverhältnismäßigen Aufwand darstellen. Urteil v. 11.12.2019, Aktenzeichen II SA / Wa 1030/19. [Online] 2019 [Zitiert 2020-03-20] Verfügbar unter https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sa-wa-1030-19-wyrok-wojewodzkiego-sadu-522853095

Es gibt diverse Aufbewahrungsfristen, die in den unterschiedlichen Gesetzen genannt werden. Z. B.

- Handels- und steuerrechtliche Vorgaben finden sich u. a. sowohl im Handelsgesetzbuch als auch der Abgabenordnung.
- In der Bundesrechtsanwaltsordnung finden sich Vorgaben für die Aufbewahrungsdauer von Handakten, in der Patentanwaltsordnung für Handakten von Patentanwälten.
- Der Aufbewahrungszeitraum von Patientendaten finden sich in den unterschiedlichsten Gesetzen wieder, wie beispielsweise dem Bürgerlichen Gesetzbuch (Fristen für die Patientenakte) oder im Strahlenschutzgesetz (Vorgaben bzgl. der Aufbewahrungsdauer von Röntgenbildern, digitale Bilddaten und sonstige Untersuchungsdaten).

Entsprechend Art. 17 Abs. 3 lit. b DS-GVO darf ein Verantwortlicher personenbezogene Daten nicht löschen, wenn diese Daten zur Erfüllung einer rechtlichen Verpflichtung [27], welcher der Verantwortliche unterliegt, erforderlich sind. Gesetzlich geforderte Aufbewahrungspflichten stellen eine rechtliche Verpflichtung im Sinne dieser Regelung dar: Solange ein Gesetz die Aufbewahrung der Daten verlangt, dürfen diese Daten nicht gelöscht werden. Je nach Umständen kann daraus aber resultieren, dass eine Einschränkung der Verarbeitung erfolgen muss, beispielsweise, wenn der Zweck der Verarbeitung erreicht wurde und die weitere Speicherung ausschließlich der Erfüllung der gesetzlich geforderten Aufbewahrung dient.

2.11 Landesarchivgesetze

Die Archivgesetze des Bundes und der Länder[28] regeln die Archivierung von Unterlagen sowie die Organisation des jeweiligen Archivs. Die Voraussetzung für die Aufnahme von Unterlagen in das jeweilige Archiv besteht darin, dass die Unterlagen von bleibendem Wert sein müssen: Die Unterlagen

- stellen einen bleibenden Wert für die Erforschung oder das Verständnis der deutschen Geschichte dar oder
- sichern die berechtigten Belange der Bürger oder
- beinhalten Informationen für Gesetzgebung, Verwaltung oder Rechtsprechung.

Über diese „Archivwürdigkeit“ darf nur das jeweils zuständige Archiv entscheiden. Grundsätzlich ist keine öffentliche Behörde oder Stelle befugt, eigenmächtig eine Löschung oder Vernichtung ihrer Unterlagen vorzunehmen; es besteht vielmehr eine Anbietungspflicht an das zuständige Archiv. Dies gilt grundsätzlich auch für im öffentlichen Auftrag agierende Stellen, eine Anstalt öffentlichen Rechts muss dementsprechend vor einer Löschung von Unterlagen eine entsprechende Nachfrage an das zuständige Archiv stellen, insbesondere, wenn Patienten Zeugen der Zeitgeschichte darstellen wie beispielsweise Bundes- oder Landesminister oder andere Personen des öffentlichen Lebens.

[27] Allgemein kann eine rechtliche Verpflichtung aus einer bindenden Vereinbarung oder einem Vertrag, der eine bestimmte Handlungsweise beinhaltet, resultieren. Im Rahmen der DS-GVO besteht eine rechtliche Verpflichtung jedoch nur dann, wenn die EU oder ein Mitgliedsstaat, dessen Recht der Verantwortliche unterliegt, dem Verantwortlichen durch gesetzliche Regelungen eine Pflicht auferlegt. Siehe auch ErwGr. 45 DS-GVO

[28] Eine Liste mit den Archivgesetzen der Länder sowie deren jeweiliger Fundort im Internet findet sich in Abschnitt 5.3 auf Seite 20

2.12 Europäischer Datenschutzausschuss

Gemäß Art. 70 Abs. 1 lit. d DS-GVO muss der europäische Datenschutzausschuss Leitlinien, Empfehlungen und bewährte Verfahren hinsichtlich der Löschung personenbezogener Daten bereitstellen. Dies gilt jedoch entsprechend den Vorgaben von Art. 17 Abs. 2 DS-GVO nur für durch den Verantwortlichen durch Kommunikationsdienste öffentlich gemachte personenbezogene Daten, wie beispielsweise Links sowie Kopien oder Replikationen dieser Daten. Wenngleich diese Leitlinien, Empfehlungen und bewährten Verfahren für sich genommen nicht verbindlich sind, bieten sie Anhaltspunkte, welche Maßnahmen zur Umsetzung der Pflichten aus Art. 17 DS-GVO zur Verfügung stehen und sind bei der Auswahl angemessener Maßnahmen zu berücksichtigen[29].

EDSA veröffentlichte im Dezember 2019 Leitlinien[30], wie Suchmaschinen das Recht auf Löschung umsetzen sollen.

[29] Herbst T.: Art. 58 Rn. 38. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

[30] EDSA: Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1). [Online] 2019 [Zitiert 2020-03-20] Verfügbar unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en

3 Begriffsdefinitionen / Glossar

Akteur	Urheber einer Handlung; neben natürlichen und juristischen Personen können auch Rollen oder Funktionen als Akteur agieren.
Anonymisierung	Prozess, durch den personenbezogene Daten derart irreversibel verändert werden, dass ein Betroffener nicht mehr direkt oder indirekt identifiziert werden kann (Quelle: DIN 66398 i.V.m. ISO/IEC 29100)
Audit	Systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Audit-Trail	Chronologische Aufzeichnung der Aktivitäten von Nutzern eines Informationssystems, die die getreue Wiederherstellung früherer Zustände der betreffenden Informationen ermöglicht. (Quelle: DIN CEN ISO/TS 14265)
Aufbewahrungsfrist	Zeitraum, innerhalb dessen die Objekte einer Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein müssen (Quelle: DIN 66398)
Aufzeichnung	Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt. (Quelle: DIN ISO IEC 27000)
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. (Quelle: DIN EN ISO 22600-1)
Authentizität	Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt. (Quelle: DIN ISO IEC 27000)
Autorisierung	Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen. (Quelle: DIN EN ISO 22600-1)
Beschäftigte	Beschäftigte sind 1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher, 2. zu ihrer Berufsbildung Beschäftigte, 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden), 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte, 5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten, 6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten, 7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende. Bewerberinnen und Bewerber für ein Beschäftigungs-verhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte. (Quelle: § 26 Abs. 8 BDSG)

Datenart	Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird (Quelle: DIN 66398)
Datenlöschung	Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt. (Quelle: DIN CEN ISO/TS 14265)
Delegierung	Übertragung eines Privilegs von einer Entität, die dieses Privileg besitzt, auf eine andere Entität (Quelle: DIN EN ISO 22600-1)
Datenobjekte	Elemente, die Daten enthalten, wie z. B. Dateien, Dokumente, Datensätze oder Attribute (Quelle: DIN 66398)
Dokument	a) Als Einheit gehandhabte Zusammenfassung oder Zusammenstellung von Informationen, die nicht-flüchtig auf einem Informationsträger gespeichert sind b) Festgelegte und strukturierte Menge von Informationen, die als Einheit verwaltet und zwischen Anwendern und Systemen ausgetauscht werden kann (Quelle: DIN 06789)
Drittland	Land, welches nicht an die gesetzlichen Anforderungen der EU-Datenschutz-Direktive gebunden ist (Land außerhalb des EWR) (Quelle: DIN EN 14484)
Einhaltung	Handlung, die erforderlich ist, um eine festgelegte Anforderung zu erfüllen (Quelle: DIN CEN ISO/TS 14441)
Elektronisches Archiv	Sammlung von Dokumenten in einem Speicher für historische Zwecke oder als Sicherungsmaßnahme. (Quelle: DIN 06789)
Entität	Natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Entpersonalisierung	Allgemeine Bezeichnung für jeden Prozess, bei dem der Bezug eines identifizierenden Datensatzes auf die betreffende Person aufgehoben wird (Quelle: DIN CEN ISO/TS 14265)
Ereignis	Auftreten von ungewöhnlichen Umständen (Quelle: DIN ISO IEC 27000)
Freigabe	a) Eine bestimmten Anweisungen entsprechende Genehmigung nach abgeschlossener Prüfung b) Formelle Aktion einer autorisierten Person/Organisation, mit der ein Dokument für einen deklarierten Zweck im Prozessablauf gültig erklärt wird (Quelle: DIN 06789)
Genehmigung	Bestätigung einer autorisierten Person/Organisation, dass etwas zuvor festgelegten Anforderungen entspricht. (Quelle: DIN 06789)
Identifikation	Erkennung einer Person in einem bestimmten Bereich mithilfe einer Reihe ihrer Attribute. (Quelle: DIN CEN ISO/TS 14441)

Identifizierbare Person	Person, die direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder Mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind. (Quelle: DIN EN 14484)
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen. (Quelle: DIN EN ISO 22600-1)
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert wird. (Quelle: DIN EN ISO 22600-2)
Konformitätsbewertung	Darlegung(en), dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Leitlinie	Vom Management formell ausgedrückte Gesamtintention und -richtung (Quelle: DIN ISO IEC 27000)
Löschung	Prozess, durch den personenbezogene Daten derart irreversibel verändert werden, dass diese nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können (Quelle: DIN 66398)
Löschfrist	Zeitraum, nach dessen Ablauf ein spezifischer Datenbestand gelöscht werden soll (Quelle: DIN 66398)
Löschklasse	Kombination aus einer Standardlöschfrist und einem abstraktem Startzeitpunkt für den Fristlauf (Quelle: DIN 66398)
Löschkonzept	Festlegungen, mit denen eine verantwortliche Stelle sicherstellt, dass ihre personenbezogenen Datenbestände rechtskonform gelöscht werden (Quelle: DIN 66398)
Löschregel	Kombination aus Löschfrist und konkreter Bedingung für den Startzeitpunkt des Fristlaufs (Quelle: DIN 66398)
Richtlinie	Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen (Quelle: DIN ISO IEC 27000)
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen (Quelle: DIN EN ISO 22600-1)
Schreddern	Mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe (Quelle: DIN EN 15713)
Sicheres Drittland	Land, dessen Gesetzgebung den Anforderungen der EU-Datenschutz-Direktive entspricht und dessen Datenschutzniveau von der Europäischen Kommission als angemessen erkannt wurde (Quelle: DIN EN 14485)
Verfahren	Festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: DIN ISO IEC 27000)

Vernichtung	Reduzierung der Größe, wodurch die Unterlagen so weit wie möglich unlesbar, unleserlich und nicht rekonstruierbar gemacht werden (Quelle: DIN EN 15713)
Zerfasern	Mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe auf mechanische Weise, kleinere Größen als mittels Schreddern erreichbar (Quelle: DIN EN 15713)

4 Abkürzungen

Abs.	Absatz
ADV	Auftragsdatenverarbeitung; alter Begriff für → AVV
AO	Abgabenordnung
Art.	Artikel
Artt.	Artikel (Mehrzahl)
AVV	Vertrag zur Verarbeitung im Auftrag („Auftragsverarbeitungsvertrag“)
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BVerfG	Bundesverfassungsgericht
bvitg	Bundesverband Gesundheits-IT e. V.
DIN	Deutsche Institut für Normung e. V.
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EN	Europäische Norm
ErwGr	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union (Europäische Gerichtshof)
EWR	Europäischer Wirtschaftsraum
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
h.M.	Herrschende Meinung
i.V.m.	In Verbindung mit
HGB	Handelsgesetzbuch
IS	Informationssystem
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap.	Kapitel
KAS	Klinisches Arbeitsplatzsystem
KHG	Krankenhausgesetz
KIS	Krankenhaus-Informationssystem
KMU	Kleines, mittelständisches Unternehmen
LDSG	Landesdatenschutzgesetz
LIS	Labor-Informationssystem
lit.	littera (lat. „Buchstabe“)
LKHG	Landeskrankenhausgesetz
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
Nr.	Nummer
ÖOGH	Österreichische Oberste Gerichtshof
OID	Objektbezeichner (en: Object Identifier)
OWiG	Gesetz über Ordnungswidrigkeiten
PACS	Picture Archiving and Communication System
PDMS	Patientendatenmanagementsystem
pbD	personenbezogene Daten

RIS	Radiologisches Informationssystem
RL	Richtlinie
Rn.	Randnummer
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TFG	Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz)
TK	Telekommunikation(s-)
Ziff.	Ziffer

5 Weiterführende Literatur

5.1 Empfehlungen

- Bundesamt für Sicherheit in der Informationstechnik: Grundschutz-Kompendium, CON.6 Löschen und Vernichten. [Online] 2020 [Zitiert 2020-03-24] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html
- bitkom: Leitfaden zum sicheren Datenlöschen. [Online] 2008 [Zitiert 2020-03-24] https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-zum-Sicheren-Datenloeschen.html bzw. pdf-Datei unter https://www.bitkom.org/sites/default/files/file/import/080602-Sicheres-Datenloeschen-Version-2-0-vom-300508.pdf
- KrollOntrack: Sichere und endgültige Datenlöschung. [Online] 2016 [Zitiert 2020-03-24] https://assets.krollontrack.com/hv3/PDF/de/ebook_datenloeschung-2017-final.pdf

5.2 Datenschutz-Aufsichtsbehörden

- Europäische Datenschutzausschuss (EDSA): Guidelines 5/2019on the criteria of theRight to be Forgotten in the search engines cases under the GDPR (part 1). [Online] 2019 [Zitiert 2020-04-23] Verfügbar unter https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf
- Artikel-29-Datenschutzgruppe: WP 225 „Leitlinien für die Umsetzung des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-131/12 „Google Spanien und Inc/Agenda Española de Protección de Datos (AEPD) und Mario Costeja Gonzáles“. [Online] 2014 [Zitiert 2020-04-23] Verfügbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236
- Datenschutzkonferenz (DSK): Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“. [Online] 2018 [Zitiert 2020-04-23] Verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf
- Landesbeauftragte für den Datenschutz Niedersachsen: Hilfestellungen für Verantwortliche bei der Festlegung von Löschfristen. [Online] 2018 [Zitiert 2020-04-23] Verfügbar unter https://lfd.niedersachsen.de/startseite/technik_und_organisation/festlegung_von_loschfristen_im_offentlichen_bereich/hilfestellungen-fuer-verantwortliche-bei-der-festlegung-von-loeschfristen-168232.html bzw. pdf-Datei unter https://lfd.niedersachsen.de/download/135513/Uebersicht_Loeschfristen.pdf
- Bayerisches Landesamt für Datenschutzaufsicht: Löschung. [Online] 2019 [Zitiert 2020-04-23] Verfügbar unter https://www.lda.bayern.de/de/thema_loeschung.html

5.3 Landesarchivgesetze

- Baden Württemberg
    - Gesetz: Gesetz über die Pflege und Nutzung von Archivgut (Landesarchivgesetz - LArchG)
    - URL: http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=ArchivG+BW&psml=bsbawueprod.psml&max=true&aiz=true
    - Normadressaten: Behörden, Gerichte und sonstige Stellen des Landes sowie deren Funktionsvorgängern oder von Rechtsvorgängern des Landes

- Bayern
    - Gesetz: Bayerisches Archivgesetz (BayArchivG)
    - URL: https://www.gesetze-bayern.de/Content/Document/BayArchivG
    - Normadressaten: Behörden, Gerichte und sonstigen öffentlichen Stellen des Freistaates Bayern
- Berlin
    - Gesetz: Gesetz über die Sicherung und Benutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin - ArchGB)
    - URL: http://gesetze.berlin.de/jportal/?quelle=jlink&query=ArchG+BE&psml=bsbeprod.psml&max=true&aiz=true
    - Normadressaten: Behörden, Gerichte und sonstigen Stellen des Landes Berlin sowie deren Rechts- und Funktionsvorgängern
- Brandenburg
    - Gesetz: Gesetz über die Sicherung und Nutzung von öffentlichem Archivgut im Land Brandenburg (Brandenburgisches Archivgesetz - BbgArchivG)
    - URL: https://bravors.brandenburg.de/gesetze/bbgarchivg
    - Normadressaten: Verfassungsorgane, Behörden, Gerichte, juristische Personen des öffentlichen Rechts oder deren Vereinigungen sowie deren Rechts- und Funktionsvorgängern oder sonstigen Stellen des Landes
- Bremen
    - Gesetz: Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Bremen (Bremisches Archivgesetz - BremArchivG -)
    - URL: https://www.transparenz.bremen.de/sixcms/detail.php?gsid=bremen2014_tp.c.128932.de&asl=bremen02.c.732.de&template=20_gp_ifg_meta_detail_d
    - Normadressaten: Behörden, Gerichte und sonstige Stellen des Landes und der Stadtgemeinde Bremen
- Hamburg
    - Gesetz: Hamburgisches Archivgesetz (HmbArchG)
    - URL: http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?doc.id=jlr-ArchivGHArahmen&st=lr&doctyp=BSBayern&showdoccase=1&paramfromHL=true#focuspoint
    - Normadressaten: Verfassungsorgane, Gerichte, Behörden und sonstigen Stellen der Freien und Hansestadt Hamburg und der ihrer Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts
- Hessen
    - Gesetz: Hessisches Archivgesetz
    - URL: https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-ArchivGHE2012V1P5
    - Normadressaten: Verfassungsorgane, Behörden, Gerichte, der Landtag und sonstige öffentlichen Stellen des Landes, der Städte, Gemeinden, Landkreise und kommunalen Verbände, ihrer Rechts- und Funktionsvorgänger sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen einschließlich der Hochschulen

- Mecklenburg-Vorpommern
    - Gesetz: Archivgesetz für das Land Mecklenburg-Vorpommern (Landesarchivgesetz - LArchivG M-V)
    - URL: http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?doc.id=jlr-ArchivGMVrahmen&st=lr&doctyp=BSBayern&showdoccase=1&paramfromHL=true#focuspoint
    - Normadressaten: Verfassungsorganen, Behörden, Gerichte und sonstigen Stellen des Landes, juristische Personen des öffentlichen Rechts und ihren Vereinigungen, die der Aufsicht des Landes unterstehen, sowie Funktionsvorgänger der genannten Stellen
- Niedersachsen
    - Gesetz: Gesetz über die Sicherung und Nutzung von Archivgut in Niedersachsen (Niedersächsisches Archivgesetz - NArchG)
    - URL: http://www.voris.niedersachsen.de/jportal/?quelle=jlink&query=ArchivG+ND&psml=bsvorisprod.psml&max=true
    - Normadressaten: Behörden, Gerichte und sonstigen Stellen des Landes sowie Stiftungen privaten Rechts, wenn das Land oder einer seiner Rechtsvorgänger überwiegend das Stiftungsvermögen bereitgestellt hat, und anderer juristischer Personen des Privatrechts, wenn sie nicht am Wettbewerb teilnehmen und dem Land mehr als die Hälfte der Anteile oder der Stimmen zusteht
- Nordrhein Westfalen
    - Gesetz: Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Nordrhein-Westfalen (Archivgesetz Nordrhein-Westfalen - ArchivG NRW)
    - URL: https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000338
    - Normadressaten: Träger der kommunalen Selbstverwaltung, deren Verbände sowie kommunalen Stiftungen sowie anderer der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts
- Rheinland-Pfalz
    - Gesetz: Landesarchivgesetz (LArchG)
    - URL: http://landesrecht.rlp.de/jportal/portal/t/ax1/page/bsrlpprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=2&numberofresults=20&fromdoctodoc=yes&doc.id=jlr-ArchivGRPrahmen&doc.part=X&doc.price=0.0&doc.hl=1#focuspoint
    - Normadressaten: Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes, der kommunalen Gebietskörperschaften und der sonstigen, der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen sowie deren Funktions- oder Rechtsvorgängern, weiterhin juristischen Personen des Privatrechts und ihre Vereinigungen, die öffentliche Aufgaben erfüllen und nicht am Wettbewerb teilnehmen
- Saarland
    - Gesetz: Saarländisches Archivgesetz (SArchG)
    - URL: http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/ArchivG_SL_rahmen.htm

    - Normadressaten: Verfassungsorgane, Behörden, Gerichte, Gemeinden und Gemeindeverbände und sonstigen öffentlichen Stellen sowie natürliche oder juristische Personen des privaten Rechts
- Sachsen
    - Gesetz: Archivgesetz für den Freistaat Sachsen (SächsArchivG)
    - URL: https://www.revosax.sachsen.de/vorschrift/2628-SaechsArchivG
    - Normadressaten: Landtag, Gerichte, Behörden und sonstigen öffentlichen Stellen, natürliche Personen oder juristische Personen des Privatrechts
- Sachsen-Anhalt
    - Gesetz: Archivgesetz Sachsen-Anhalt (ArchG LSA)
    - URL: https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-ArchGST1995V6P6
    - Normadressaten: Verfassungsorgane, Behörden, Gerichte und sonstige öffentlichen Stellen des Landes Sachsen-Anhalt, Gemeinden, Verbandsgemeinden und Landkreise sowie sonstige kommunale Zusammenschlüsse und sonstige der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Zusammenschlüssen sowie deren Rechts- und Funktionsvorgängern
- Schleswig-Holstein
    - Gesetz: Gesetz über die Sicherung und Nutzung öffentlichen Archivgutes in Schleswig-Holstein (Landesarchivgesetz - LArchG)
    - URL: http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=ArchivG+SH&psml=bsshoprod.psml&max=true
    - Normadressaten: Behörden und Gerichte des Landes, deren Organisationseinheiten sowie ihrer Funktionsvorgänger und der Rechtsvorgänger
- Thüringen
    - Gesetz: Thüringer Gesetz über die Sicherung und Nutzung von Archivgut (Thüringer Archivgesetz -ThürArchivG-)
    - URL: http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=ArchivG+TH&psml=bsthueprod.psml&max=true
    - Normadressaten: Verfassungsorgane, Behörden, Gerichte und sonstige Stellen des Landes, bei deren Funktions- und Rechtsvorgängern sowie sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen sowie Gemeinden, Landkreise, juristische Personen des öffentlichen Rechts, die deren Aufsicht unterstehen, sowie deren Funktions- und Rechtsvorgängern

5.4 Normen

- DIN EN 15713: Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln. Stand: 2009-08
- DIN 66398: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Stand: 2016-05
- DIN 66399-1: Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe . Stand: 2012-10
- DIN 66399-2: Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern . Stand: 2012-10
- DIN SPEC 66399-3: Vernichten von Datenträgern - Teil 3: Prozess der Datenträgervernichtung. Stand: 2013-02

- DIN EN ISO/IEC 27040: IT-Sicherheitsverfahren - Speichersicherheit . Stand: 2017-03
- ISO/IEC 21964-1: Destruction of data carriers - Part 1: Principles and definitions. Stand: 2018-08
- ISO/IEC 21964-2: Destruction of data carriers - Part 2: Requirements for equipment for destruction of data carriers. Stand: 2018-08
- ISO/IEC 21964-3: Destruction of data carriers - Part 3: Process of destruction of data carriers. Stand: 2018-08

5.5 Bücher

- Becker C. Das Recht auf Vergessenwerden. Mohr Siebeck, 1. Auflage 2019. ISBN 978-3-16-156456-7, DOI 10.1628/978-3-16-156457-4
- Hunzinger S. Das Löschen im Datenschutzrecht. Nomos Verlagsgesellschaft, 1. Auflage 2018. ISBN 978-3-8487-5196-9, DOI 10.5771/9783845293912-1
- Milker J. Die Umsetzung des „Rechts auf Vergessenwerden“ im deutschen Recht: Der Datenschutz als Taktgeber für das Äußerungsrecht. Springer, 1. Auflage 2019. ISBN 978-3-658-28141-0, DOI 10.1007/978-3-658-28142-7
- Werro, Franz (Ed.) The Right To Be Forgotten - A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia. Springer, 1. Auflage 2020. ISBN 978-3-030-33511-3, DOI 10.1007/978-3-030-33512-0

5.6 Zeitschriften

- Abel R. (2017) Lösch- und Sperrkonzepte nach der DS-GVO. PinG: 177-182
- Berning W, Meyer K, Keppeler L. (2017) Datenschutz-konformes Löschen personenbezogener Daten in betrieblichen Anwendungssystemen - Methodik und Praxisempfehlungen mit Blick auf die EU DS-GVO. HMD: 618-631
- Conrad I, Hausen D. (2011) Datenschutzgerechte Löschung personenbezogener Daten - Verschärfung durch den Gesetzentwurf zum Beschäftigtendatenschutz. ITRB: 35-40
- Dovas M. (2017) Die Pflicht zur Löschung von Daten: Änderungen durch die DS-GVO und Umsetzung im Unternehmen. ITRB: 186-191
- Dralle T. 2017) Recht auf Löschung: Der Radiergummi der DS-GVO. BvD-News: 46-49
- Durmus E, Selzer A, Pordesch U. (2019) Das Löschen nach der DS-GVO - Eine Diskussion der datenschutzkonformen Umsetzung bei E-Mails. DuD: 786-791
- Fraenkel R, Hammer V. (2007) Rechtliche Löschvorschriften. DuD: 899-904
- Greveler U, Wegener C. (2010) Ein Ansatz zur Umsetzung von Löschvorschriften mittels Verschlüsselung. DuD: 467-471
- Grimm D, Kühne J. (2018) Löschkonzept nach der DS-GVO - Alle Aufbewahrungspflichten und -rechte sowie Löschfristen bei Beschäftigtendaten im Überblick. ArbRB: 144-149
- Gründel A. (2019) Ermittlung des Löschbedarfs bei unstrukturierten Datenbeständen - Eine praxisnahe Herangehensweise für die routinemäßige Datenlöschung. ZD: 493-497
- Hammer V, Fraenkel V. (2007) Löschkonzept. DuD: 905-910
- Hammer V, Fraenkel V. (2011) Löschklassen - Standardisierte Fristen für die Löschung personenbezogener Daten. DuD: 890-895
- Hennemann M. (2016) Das Recht auf Löschung gemäß Art. 17 Datenschutz-Grundverordnung. PinG: 176-179
- Hunzinger S. (2018) Löschkonzepte nach der DS-GVO am Beispiel von ERP-Systemen. CR: 357-366
- Jacobi J, Jantz M. (2017) Löschpflichten nach der EU-Datenschutzgrundverordnung - Was Arbeitgeber jetzt bereits tun müssen. ArbRB: 22-26

- Kalabis L, Selzer A. (2012) Das Recht auf Vergessenwerden nach der geplanten EU-Verordnung. DuD: 670-675
- Katko P, Knöpfle K, Kirschner T. (2014) Archivierung und Löschung von Daten - Unterschätzte Pflichten in der Praxis und ihre Umsetzung. ZD: 238-241
- Keppeler L, Berning W. (2017) Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten - Anforderungen an Löschkonzepte und Datenbankstrukturen. ZD: 314-319
- Keppeler L. (2018) Das „Radierverbot“ als „Rettung“ vor den umfangreichen DS-GVO-Löschpflichten. RDV: 70-75
- Klickermann P. (2018) Die Privilegierung des Löschungsrechts - Das Recht auf Vergessenwerden im Fokus der beruflichen Tätigkeit. MMR: 209-212
- Kodde C. (2013) Die „Pflicht zu Vergessen” - „Recht auf Vergessenwerden” und Löschung in BDSG und DS-GVO. ZD: 115-118
- Knuchel C, Ebert N. (2020) DSGVO-konformes Löschen. DuD: 126-127
- Kühling J, Klar M (2014) Löschpflichten vs. Datenaufbewahrung Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten. ZD: 506-510
- Kühling J. (2020) Das „Recht auf Vergessenwerden“ vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem. NJW: 275-280
- Padova Y. (2019) Is the right to be forgotten a universal, regional, or ‘glocal’ right? IDPL: 15-29
- Pörschke V, Wilhelm W. (2018) Kampfansage an die Datenkraken - Das System der Löschpflichten der DS-GVO. PinG: 88-92
- Riesenhuber K. (2014) Der Einsichts- und Löschungsanspruch nach §§ 34, 35 BDSG im Beschäftigungsverhältnis - Am Beispiel der Personalakten. ZD: 753-757
- Stiemerling O. (2018) Löschen: Mission Impossible? PinG: 93-96

Teil II: Aufbau und Struktur eines Löschkonzeptes

Entsprechend Art. 5 Abs. 1 i. V. m. ErwGr. 39 DS-GVO hat der Verantwortliche Fristen für die Löschung personenbezogener Daten festzulegen sowie eine regelmäßige Überprüfung bzgl. anstehender Löschungen vorzusehen: Es existiert eine Prüfpflicht des Verantwortlichen[31].

1 Grundlegender Aufbau

Die Gliederung eines Löschkonzeptes kann wie folgt aussehen:

1. Geltungs- und Anwendungsbereich des Löschkonzeptes
2. Definition von Datenarten/-kategorien und den für sie geltenden gesetzlichen Aufbewahrungsfristen
3. Abwägung von Lösch- und Aufbewahrungsinteressen
4. Prozessbeschreibung
    a. Festlegung der Verantwortlichkeiten
        i. Geschäftsführung, welche die Gesamtverantwortung besitzt
        ii. Datenverantwortliche, welche die Löschpflicht prüfen und falls erforderlich die Löschung anweisen
        iii. Systemverantwortliche, welcher die Löschung durchführen
        iv. Auditverantwortliche, welche die Einhaltung der Vorgaben prüfen
    b. Umgang mit individuellen Löschanträgen durch betroffene Personen
    c. Einzuhaltende Vorgehensweisen bzw. Standards bei der Löschung insbesondere auch Protokollierung der Löschung
        i. Löschzeiten
        ii. Löschverfahren
        iii. Einschränkung der Verarbeitung
        iv. Löschprotokoll
    d. Umgang mit Archiven und Sicherungskopien
    e. Überprüfung der Einhaltung des Löschkonzeptes sowie Anpassungsbedarf
5. Mitgeltende Unterlagen
    a. Rollen- und Berechtigungskonzept, insbesondere Festlegung der Rechte hinsichtlich des Löschens personenbezogener Daten
6. Inkrafttreten
7. Anlage: Rechtsgrundlagen und Aufbewahrungsfristen

2 Aufbau und Struktur eines Löschkonzeptes

Im Folgenden wird in aller Kürze beschrieben, wie ein Löschkonzept aufgebaut sein kann und welche Angaben enthalten sein sollten.

[31] Herbst T.: Art. 17 Rn. 47. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung/BDSG. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-71932-5

2.1 Geltungs- und Anwendungsbereich des Löschkonzeptes

In kleineren Organisationen kann es sein, dass ein einziges Löschkonzept ausreicht. Aber selbst in kleineren Krankenhäusern werden verschiedene IT-Systeme wie beispielsweise das KIS, ein System für Transfusionswesen (z. B. für Eigenblutgaben) oder auch für das Personalmanagement vorhanden sein. Hier ist es häufig sinnvoll, dass für jedes IT-System, ein eigenes Löschkonzept existiert, da einerseits für die in den jeweiligen Systemen verarbeiteten Daten unterschiedliche Aufbewahrungsfristen gelten können, andererseits die IT-Systeme unterschiedliche Mechanismen für den Umgang mit den Löschpflichten bieten: während ein System beispielsweise eine Arbeitsliste bietet, in welchem an Hand von Metadaten Daten, deren Löschzeitpunkt erreicht ist, zur Abarbeitung listet, müssen in einem anderen System von in der IT-Abteilung Beschäftigten die notwendigen Informationen mittels SQL-Abfragen zusammengetragen werden. Für in Dateisystemen unstrukturiert gespeicherte personenbezogene Daten wiederum werden Beschäftigte der IT-Abteilung keine Listen erstellen können, vielmehr müssen die erstellenden Organisationseinheiten selbst in die Pflicht genommen werden.

In diesen größeren Organisationen/Unternehmen bietet es sich an, ein Rahmen-Löschkonzept zu erstellen, in welchem die grundlegenden, für alle gleichermaßen geltenden Regelungen enthalten sind, wie beispielsweise die Darstellung der Löschpflicht, die Festlegung der Verantwortlichkeiten oder auch der Umgang mit Löschanträgen betroffener Personen wie Beschäftigte oder Patienten. In den Löschkonzepten für die jeweiligen IT-Systeme wird dann Bezug auf das Rahmen-Löschkonzept und dessen ergänzende Geltung festgehalten; ergänzend werden die Regelungen aufgenommen, die speziell für dieses IT-System gelten: also beispielsweise die Datenarten/-kategorien bestimmt oder wie wann welche Daten gelöscht werden.

In allen Löschkonzepten muss aber der jeweilige Geltungs- und Anwendungsbereich festgelegt sein, denn nur wenn Anwender eine hinreichende Klarheit haben, was wann wie aus welchen Gründen von wem zu löschen ist, können die Beschäftigten auch entsprechend agieren.

Dementsprechend würde in einem Rahmenlöschkonzept festgehalten, dass der Geltungs- und Anwendungsbereich für das gesamte Krankenhaus gilt, in einem Löschkonzept für ein PACS hingegen der Geltungs- und Anwendungsbereich auf die im Krankenhaus befindlichen Fachabteilungen eingeschränkt ist, welche die Daten in ein PACS einstellen. Grundüberlegung bei den IT-System-bezogenen Löschkonzepten ist, dass immer die die personenbezogene Daten erzeugende Fachinstanz (beispielsweise Herzchirurgie) das notwendige Wissen hat, um die Entscheidung bzgl. des Lebenszyklus treffen zu können; i. d. R. hat nur die Fachinstanz das für die Darstellung des Lebenszyklus erforderliche Wissen bzgl. der gesetzlichen Aufbewahrungsvorgaben. Dementsprechend sind bei der Erstellung von IT-System-bezogenen Löschkonzepten auch immer alle beteiligten Fachinstanzen einzubeziehen, damit die im System verarbeiteten Datenarten/-kategorien sowie die dazugehörigen Lebenszyklen definiert werden.

Der erste Schritt bei der Erstellung eines Löschkonzeptes ist daher die Festlegung des Geltungs- und Anwendungsbereichs, wobei dadurch zugleich die einzubeziehenden Fachbereiche definiert werden.

2.2 Definition von Datenarten/-kategorien und den für sie geltenden gesetzlichen Aufbewahrungsfristen

Es müssen alle personenbezogenen Daten aufgeführt werden. Gerade im medizinischen Umfeld kann natürlich nicht jedes einzelne Datum benannt werden, vielmehr müssen eindeutige Bezeichnungen

für Datenarten bzw. Datenkategorien gewählt werden, die letztlich einerseits für die das Löschkonzept anwendenden Beschäftigten verständlich sind, andererseits auch die gesetzlichen Anforderungen abbilden.

Beispielsweise werden in § 14 TFG Aufbewahrungszeiten für Blutprodukte und von Arzneimittel zur spezifischen Therapie von Gerinnungsstörungen bei Hämophilie genannt. Dementsprechend würde man in einem Löschkonzept entsprechende Datenkategorien abbilden, nicht jedoch die Pharma- oder Handelsnamen der jeweiligen Produkte auflisten. Zugleich werden die gesetzlichen Aufbewahrungsvorgaben festgehalten. Eine entsprechende Darstellung kann wie folgt aussehen:

Nr.	Datenart/-kategorie	Personengruppe	Verwendungszweck	Aufbewahrungsfrist	Rechtsgrundlage
1	Stammdaten	Patienten	Abrechnung	10 Jahre	§ 630f BGB § 10 Abs. 3 MBO-Ä 1997
2	Arbeitszeit-nachweise	Beschäftigte	Nachweis Arbeitszeit	2 Jahre	§ 16 Abs. 2 S. 2 ArbZG
3	Löschprotokolle	Beschäftigte	Nachweis der Löschung pbD	Bis zum Ende des auf der Generierung folgenden Jahres	keine

Aufbewahrungsfristen beinhalten implizit die Verpflichtung zur Löschung, wenn keine andere rechtliche Grundlage für eine weitere Verarbeitung und insbesondere Speicherung existiert. D. h. es existieren mehr oder weniger feste Fristen für die Löschung, die nur einen engen Spielraum für den Verantwortlichen beinhalten. Die fachlichen Prozesse beim jeweiligen Verantwortlichen sind dann so zu gestalten, dass die gesetzlich vorgegebenen Fristen regelhaft eingehalten werden.

Einige Vorgaben sind aber auch dynamisch. Beispielsweise schreibt § 630f BGB, analog zu § 10 Abs. 3 MBO-Ä, eine Aufbewahrung der Patientenakte „für die Dauer von zehn Jahren nach Abschluss der Behandlung“ vor, d. h. Beginn der „Zeitrechnung“ ist der Abschluss der Behandlung, wobei „Abschluss der Behandlung“ nicht das Ende der Arzt-Patienten-Beziehung bedeutet, sondern wenn die Behandlung eines Krankheitsvorganges (durch den Arzt resp. der Arztpraxis bzw. des Krankenhauses) abgeschlossen ist[32]. Dies ist gerade im medizinischen Kontext schwierig, da Patientenakten regelhaft nicht für die einzelne Erkrankung geführt werden, sondern im vollständigen Behandlungskontext. Dennoch muss im Zweifelsfall nachgewiesen werden, ob Informationen aus einem abgeschlossenen Behandlungsfall für eine neue Behandlung genutzt wurden, sodass der „alte“ Behandlungsfall als zur Dokumentation der neuen Behandlung zugehörig gerechnet werden kann und somit die gesetzliche Aufbewahrungsdauer neu zu zählen beginnt.

2.3 Abwägung von Lösch- und Aufbewahrungsinteressen

Mitunter kommt es vor, dass Daten über den vom Gesetzgeber vorgegebenen Aufbewahrungszeitraum hinaus gespeichert werden sollen. Auch hierfür sind sowohl eine Rechtsgrundlage wie auch die Benennung des Zweckes zwingend erforderlich. Wie in Teil I, Abschnitt 2.3.2 auf Seite 6 dargestellt, kann ein entsprechender Zweck die Verwendung der Daten für eine bevorstehende oder bereits stattfindende gerichtliche Auseinandersetzung sein. Aber auch

[32] So z. B.:
- Holzner C. Aufbewahrung der Krankenunterlagen. In: Holzner C. (2020) Datenschutz, Dokumentations- und Organisationspflichten in der ärztlichen Praxis. C. H. Beck Verlag, 1. Auflage. ISBN: 978-3-406-73799-2

andere Verarbeitungszwecke sind natürlich vorstellbar wie beispielsweise die Nutzung der Daten für Forschung.

Ist eine entsprechende Speicherung vorgesehen, so ist der jeweilige Zweck anzugeben und die Rechtsgrundlage, welche die Verarbeitung der personenbezogenen Daten zu diesem Zweck erlaubt, darzustellen. In der Regel wird hier eine Interessenabwägung zwischen den Interessen des Verantwortlichen an einer weiteren Verarbeitung sowie den Interessen der betroffenen Personen erforderlich sein.

2.4 Prozessbeschreibung

2.4.1 Festlegung der Verantwortlichkeiten

2.4.1.1 Geschäftsführung, welche die Gesamtverantwortung besitzt

Grundsätzlich liegt die Erfüllungspflicht der rechtlichen Anforderung des Löschens beim Verantwortlichen, i. d. R. also dem Inhaber des Unternehmens bzw. der Organisation bzw. der Geschäftsführung. Im Rahmen des Direktionsrechts können und sollten Aufgaben aber an Bereiche adressiert werden, welche die festgelegten Prozesse umsetzen.

Im Rahmen eines Rahmen-Löschkonzeptes oder auch bei der Erstellung eines einzelnen Löschkonzeptes liegt also – ähnlich wie im Qualitätsmanagement – die Gesamtverantwortung bei der Unternehmensleitung und dies sollte im Löschkonzept auch festgehalten werden.

2.4.1.2 Datenverantwortliche, welche die Löschpflicht prüfen und falls erforderlich die Löschung anweisen

Die Information, welche gesetzlichen Rahmenbedingungen hinsichtlich Aufbewahrungspflichten gelten, liegen in der Regel bei der jeweiligen Fachabteilung: die Personalabteilung wird die Aufbewahrungsfristen für Personaldokumente kennen, die Chefärzte müssen um die Aufbewahrungspflichten für die medizinische Dokumentation wissen. Verantwortlich für ihre jeweiligen Bereiche sind demnach die jeweiligen Leitungen, auch dies sollte im Löschkonzept festgehalten werden.

Aber auch die Leitungen der jeweiligen Abteilungen bzw. Kliniken werden im Tagesgeschäft womöglich so viel zu tun haben, dass sie sich selbst um das Thema „Löschen“ nicht hinreichend kümmern können. Daher sollte seitens der Leitungen Personen als Verantwortliche benannt werden, die das Thema „Löschen“ als Aufgabe zugewiesen bekommen. Diese „Datenverantwortlichen“ sind die Personen, welche inhaltlich entscheiden müssen, welche Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist gelöscht werden oder auch nicht. Zu den Aufgaben der Datenverantwortlichen gehört dann ggf. auch, Beschäftigte der IT-Abteilung mit der Löschung personenbezogener Daten zu beauftragen[33].

2.4.1.3 Systemverantwortliche, welche die Löschung durchführen

Datenverantwortliche können nicht zwangsläufig auch Daten löschen. Nicht jede Person, welche inhaltlich über einen Löschvorgang entscheiden kann, hat das notwendige IT-Wissen, um eine Löschung auch durchführen zu können; ggf. müssen individuelle SQL-Kommandos erstellt werden.

[33] Im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag müssen ggf. entsprechende Weisungsbefugnisse vorgesehen werden, wenn derartige Aufträge dem Auftragsverarbeiter erteilt werden sollen. Alternativ sind entsprechende Pflichten direkt im Vertrag zur Auftragsverarbeitung zu integrieren.

Neben den Datenverantwortlichen sollten daher auch Systemverantwortliche ernannt werden. Systemverantwortliche führen einerseits die Löschung technisch aus, andererseits sorgen sie dafür, dass den Datenverantwortlichen Listen vorgelegt werden, an Hand derer entscheiden werden kann, welche Daten gelöscht werden müssen und welche noch weiter gespeichert werden sollen. Es spricht aber nichts dagegen, dass bei entsprechender Eignung die Position des Daten- und die des Systemverantwortlichen durch eine Person besetzt wird.

2.4.1.4 Auditverantwortliche, welche die Einhaltung der Vorgaben prüfen

Art. 32 Abs. 1 lit. d DS-GVO schreibt ein Verfahren „zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“, mithin auch der Umsetzung der Löschpflichten. Daher muss in regelmäßigen, vom Verantwortlichen festzulegenden Abständen auch die Einhaltung der Vorgaben des Löschkonzeptes bzw. der Löschkonzepte geprüft werden. Dies kann als eigenständige Prüfung z. B. durch den Datenschutzbeauftragten erfolgen, aber ebenso gut im Rahmen von anderen Audits wie z. B. QM-Audits oder IT-Sicherheits-Audits erfolgen.

Existiert ein Datenschutzbeauftragter in der Organisation/im Unternehmen, so gehört nach Art. 39 Abs. 1 lit. b DS-GVO die Überwachung der Einhaltung der DS-GVO zu den gesetzlich vorgegebenen Pflichten des Datenschutzbeauftragten, sodass dieser jederzeit unabhängig von Auditvorgaben eine entsprechende Überprüfung der Löschvorgaben durchführen darf.

2.4.2 Umgang mit individuellen Löschanträgen durch betroffene Personen

Für den Umgang mit Betroffenenanfragen muss in der Organisation/Unternehmen ein Prozess etabliert sein, dies gilt selbstverständlich auch für den Umgang mit Löschanträgen einer betroffenen Person.

Zu diesem Prozess gehört zunächst die Identifizierung der „Entry-Points“, d. h. der Punkte, an denen Anfragen eingehen können. Hierzu können z. B. Telefonzentrale, Kontaktformular Internet, E-Mail-Kommunikationsadressen des Unternehmens, wie sie sich beispielsweise im Impressum befinden, usw. gehören; es gibt keine formale Vorgabe, wie eine betroffene Person mit einem Unternehmen Kontakt aufnimmt, sondern die betroffene Person ist hier in ihrer Wahl frei.

Wurden die Entry-Points identifiziert, so ist das dort eingesetzte Personal, d. h. die die Anfragen entgegennehmenden Personen, bzgl. dieser Entgegennahme zu schulen: Welche Informationen müssen erfragt werden? An wen wird die Anfrage weitergeleitet?

Dabei werden diejenigen, welche die Betroffenenanfrage entgegennehmen, i. d. R. nicht diejenigen sein, welche die Anfrage auch bearbeiten. Aber die Personen, welche die Erstbearbeitung übernehmen, müssen eine Eingangsprüfung vornehmen:

- Überprüfung, ob es sich tatsächlich um eine datenschutzrechtliche Anfrage handelt
- Erfassung der Anfrage in einem geeigneten Dokumentationssystem
- Überprüfung, worum es sich handelt
  (Auskunftsersuchen, Korrekturanfrage, Löschungsersuchen, …)
- Versendung einer Eingangsbestätigung an den Antragssteller
- Prüfung der Identität des Antragsstellers
- Prüfung, ob
  - unbegründete Antrag i.S.v. Art. 12 Abs. 5 DS-GVO
  - exzessiven Anträgen einer betroffenen Person vorliegen.

Kann der Antrag nicht sofort bearbeitet werden, muss bei der Erstbearbeitung direkt (=ohne Verzögerung) eine Information an die betroffene Person gesendet werden, worin ihr die Verzögerung inkl. der Gründe dafür erläutert werden.

Nach dieser Eingangsprüfung erfolgt eine inhaltliche Prüfung, welche z. B. beinhaltet:

- Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet werden/wurden.
- Wenn keine Daten vorhanden sind: Negativmitteilung an den Betroffenen versenden.
- Bei Löschungsersuchen erfolgt eine Weiterleitung an den zuständigen Datenverantwortlichen.
- Sobald Umsetzung erfolgt eine Information der betroffenen Person.

Im Prozessablauf ist zu beachten, dass alle Anfragen betroffener Personen unverzüglich, spätestens aber innerhalb von 4 Wochen, zu bearbeiten sind. (Siehe hierzu auch Abschnitt 2.4 auf Seite 8)

2.4.3 Einzuhaltende Vorgehensweisen bzw. Standards bei der Löschung insbesondere auch Protokollierung der Löschung

2.4.3.1 Löschzeiten

Im Löschkonzept sollte sowohl festgelegt werden*, ab wann* Daten *gelöscht werden dürfen*, als auch *bis wann* Daten *gelöscht sein müssen*. D. h. Löschregeln sollten eine Löschfrist beinhalten, die dementsprechend einen Startzeitpunkt und ein Ende benennt. Auch wenn die Aufbewahrungsfristen in den Gesetzen klar geregelt sind, ist es aus organisatorischer Sicht in den meisten Versorgungseinrichtungen nicht durchführbar, dass jeden Tag ein Datenverantwortlicher sich die Zeit zur Abarbeitung von entsprechenden Listen nehmen kann; bedingt durch die erforderliche Fachkenntnis wird der Datenverantwortliche gerade bei Gesundheitsdaten regelhaft in der Gesundheitsversorgung tätig sein und den Bereich des Datenverantwortlichen als „Nebenjob“ ausüben. Zudem ist eine taggenaue Festlegung des Löschpunktes gerade Du bei den mehrjährigen Aufbewahrungsfristen in der medizinischen Behandlung regelhaft eher nicht möglich, da das genaue Ende einer Behandlung sehr häufig nicht eindeutig bestimmt werden kann[34]: Endete die Behandlung mit der Entlassung? Oder mit dem Ende der Nachbehandlung durch die berufsgenossenschaftliche Ambulanz des Krankenhauses? Oder mit Ende der Anschluss-Heilbehandlung? § 630f BGB verlangt eine Aufbewahrung „für die Dauer von zehn Jahren nach Abschluss der Behandlung“, was rechtlich nicht mit der Entlassung aus dem Krankenhaus oder dem Ende des Abrechnungsquartals in der niedergelassenen Arztpraxis übereinstimmen muss.

Wenn Datenverantwortliche beispielsweise einmal monatlich entsprechende Listen abarbeiten, werden einige Daten sehr zeitnah gemessen am Ende der Aufbewahrungsfrist gelöscht, andere ggf. erst mit einer vierwöchigen „Verspätung“. Die Gewährleistung einer ordnungsgemäßen Zuordnung von Löschaufträgen und der damit verbundenen Überprüfung, dass nicht noch aufzubewahrende Daten gelöscht werden, bedingt eine gewissenhafte Prüfung ohne Zeitdruck, sodass eine entsprechende verzögerte Löschung dem risikobasierten Ansatz der DS-GVO Rechnung trägt.

[34] Spezialgesetze enthalten daher teilweise entsprechende Regelungen. § 4a HmbKHG beinhaltet beispielsweise die Regelung „Behandlungsunterlagen oder entsprechende elektronische Daten über Patientinnen und Patienten, die vollstationär sowie vor- und nachstationär behandelt wurden (Patientenakten), für die Dauer von 30 Jahren aufzubewahren oder zu speichern. Die Aufbewahrungs- beziehungsweise Speicherungsfrist beginnt mit Ablauf des Jahres, in dem die Behandlung abgeschlossen ist.“ Aber auch hier ist die Frage: Wann ist die Behandlung abgeschlossen?

2.4.3.2 Löschverfahren

Die Löschverfahren sollten detailliert beschrieben sein [35]. Z. B. sollte das Verfahren einer Anonymisierung detailliert dargestellt werden, inklusive dem Nachweis, dass als Ergebnis des Verarbeitungsverfahrens ein anonymisierter Datenbestand resultiert.

Für das Löschen in den eingesetzten Informationssystemen muss entsprechend den Vorgaben des Herstellers festgelegt werden, wie Löschen umzusetzen ist. Man sollte sich vom Hersteller bestätigen lassen, dass es sich bei dem Löschvorgang um einen irreversiblen Vorgang handelt.

Weiterhin müssen Regeln aufgestellt werden, wie mit anderen Dokumenten (z. B. im Dateisystem gespeicherten Briefen, Tabellenkalkulationen), E-Mails usw. umzugehen ist, gleiches gilt für Papierdokumente.

Bzgl. physikalischer Löschung sollte eine Vernichtung entsprechend DIN 66399 erfolgen. Gemäß DIN 66399-1 sind Daten von Berufsgeheimnisträgern der Schutzklasse 3 zuzuordnen, d. h. mindestens Sicherheitsstufe 4, besser jedoch Sicherheitsstufe 5 oder höher ist anzuwenden. In DIN 66399-2 finden sich dann für die jeweiligen Datenträger (z. B. Papier, Mikrofilm, CD/DVD/Blu-ray, Festplatte, SSD, Magnetbänder usw.) Vorgaben, was das Ergebnis der Vernichtung sein muss. Diesen Vorgaben entsprechend können hierzu qualifizierte Dienstleister beauftragt werden. An dieser Stelle sind jedoch etwaige gesetzliche Einschränkungen bei der Inanspruchnahme von Dienstleistern zu berücksichtigen, insbesondere Vorgaben zur örtlichen Verarbeitung in einzelnen Landeskrankenhausgesetzen.

2.4.3.3 Einschränkung der Verarbeitung („Sperrung)

Werden personenbezogene Daten für andere als dem oder den ursprünglichen Zweck(en) verwendet, wie beispielsweise zur Erfüllung gesetzlicher Aufbewahrungsfristen oder zur Ausübung bzw. Verteidigung von Rechtsansprüchen, so müssen diese Daten bzgl. ihrer Verarbeitungsmöglichkeiten dahingehend eingeschränkt werden, dass die Daten nur noch zur Erreichung dieser gesetzlich definierten Zwecke verarbeitet werden können. Dies beinhaltet i. d. R. die Sperrung der Daten für andere Zwecke, insbesondere der Zweck „Erfüllung gesetzlichen Aufbewahrungsfrist“ beinhaltet abgesehen von der Speicherung nur noch die damit verbundenen Zwecke, z. B. im Rahmen der in § 630f BGB verankerten Aufbewahrungsfrist für Patientenakten die in § 630f Abs. 2 BGB genannte „künftige Behandlung“ oder die in § 630g BGB genannte Einsichtnahme.

Art. 18 DS-GVO sieht verschiedene Fälle vor, in denen betroffene Personen eine Einschränkung der Verarbeitung verlangen können:

1) Wenn von der betroffenen Person die Richtigkeit der Daten bestritten wird, sind die Daten für die Dauer der Prüfung der Daten auf Richtigkeit zu sperren, d. h. in diesem Zeitintervall soll keine Löschung erfolgen.

[35] Hinweise finden sich z. B.:

- Grundschutz-Kompendium des BSI CON.6 Löschen und Vernichten. [Online] 2020 [Zitiert 2020-03-24] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html
- bitkom: Leitfaden zum sicheren Datenlöschen. [Online] 2008 [Zitiert 2020-03-24] https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-zum-Sicheren-Datenloeschen.html bzw. pdf-Datei unter https://www.bitkom.org/sites/default/files/file/import/080602-Sicheres-Datenloeschen-Version-2-0-vom-300508.pdf
- KrollOntrack: Sichere und endgültige Datenlöschung. [Online] 2016 [Zitiert 2020-03-24] https://assets.krollontrack.com/hv3/PDF/de/ebook_datenloeschung-2017-final.pdf

2) Erfolgte die Verarbeitung der Daten unrechtmäßig, müssen die Daten gesperrt werden, wenn die betroffene Person die Löschung ablehnt.
3) Auch sind die Daten zu sperren und nicht zu löschen, wenn der Verarbeitungszweck erreicht ist und die Daten seitens des Verantwortlichen eigentlich zu löschen sind, die betroffene Person die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.

Weiterhin kann es vorkommen, dass im Verlauf eines Rechtsstreites eine gerichtliche Anordnung die Löschung verbietet oder Daten in Gerichtsverfahren verwendet werden. Hier sind Einzelfallentscheidungen erforderlich, wie mit diesen Daten umzugehen ist.

Entsprechend müssen im Löschkonzept entsprechende Vorgaben enthalten sein, wie diese Anforderungen zur Sperrung der Daten umgesetzt werden können.

2.4.3.4 Löschprotokoll

Auch hinsichtlich der Löschpflicht besteht eine Nachweispflicht, dementsprechend muss die Löschung bzw. die Vernichtung personenbezogener Daten in geeigneter Weise protokolliert werden. Werden Auftragnehmer mit der Löschung/Vernichtung beauftragt, so sind diese zu verpflichten, dem Verantwortlichen entsprechende Löschprotokolle zu übergeben.

Ein Löschprotokoll sollte folgende Mindestinhalte enthalten:

- Datenverantwortliche Stelle (also z. B. Personalabteilung oder Gynäkologie)
- Datum und Uhrzeit der Löschung
- Für die Löschung verantwortliche Person, d. h. die/den Datenverantwortlichen (inkl. Rolle/Funktionen)
- Die ausführenden Personen (inkl. Rollen/Funktionen)
- Die Methode der Datenlöschung
- Eine Beschreibung der zu löschenden Daten, Datenarten/-kategorien
- Die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport); wurden Daten an Dritte weitergegeben ggf. entsprechendes Aktenzeichen zur Abarbeitung von Nachfragen dokumentieren, wenn gewährleistet ist, dass damit keine Person identifiziert, sondern nur die Löschung beauskunftet werden kann
- Die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport).

Das Löschprotokoll selbst darf keine der zu löschenden personenbezogenen Daten enthalten, eine Überprüfung kann ausschließlich an Hand der Beschreibung und der Anzahl der Daten erfolgen.

Das Löschprotokoll enthält aber selbst auch personenbezogene Daten der Beschäftigten, welche die Löschung durchführten. Dementsprechend müssen auch für die Löschprotokolle im Löschkonzept Löschregelungen und damit auch eine maximale Speicherdauer enthalten sein. Eine gesetzliche Vorgabe für die Speicherdauer von Löschprotokollen existiert nicht, aber im 3. Teil des BDSG, welcher der Umsetzung der Richtlinie (EU) 2016/680 dient, findet sich in § 76 Abs. 4 BDSG die Verpflichtung „Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen“. Da die Regelung für Protokolle, welche für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung angelegt wurden, gilt, kann diese Regelung, auch wenn sie nicht der Umsetzung der DS-GVO dient, im Sinne einer Analoginterpretation genutzt werden und diese Speicherdauer für Löschprotokolle angesetzt werden.

Anderer Ansatzpunkt zur Bestimmung der Speicherdauer: Nach § 41 BDSG gelten für Bußgelder, die nach Art. 83 DS-GVO verhängt werden (sollen), die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Entsprechend § 31 Abs. 2 OWiG verjährt die Verfolgung von Ordnungswidrigkeiten in drei Jahren bei Ordnungswidrigkeiten, die mit Geldbuße im Höchstmaß von mehr als fünfzehntausend Euro bedroht sind, wobei die Verjährung beginnt, sobald die Handlung beendet ist. Diese Regelung kann man dahingehend interpretieren, dass eine Aufsichtsbehörde eine Löschung nicht länger als drei Jahre verfolgen und dementsprechend auch keinen Nachweis bzgl. Löschung fordern kann. Somit wäre auch eine Speicherdauer von Löschprotokollen von drei Jahren als angemessen anzusehen.

2.4.4 Umgang mit Archiven sowie Sicherungskopien

Grundsätzlich ist im Rahmen eines Löschkonzeptes zwischen Archiven und Sicherungskopien zu unterscheiden, insbesondere dürfen durch den Verantwortlichen die Konzepte von Sicherungskopien und Archivsystemen nicht vermengt werden.

a) Archive dienen der Langzeitspeicherung. Daten werden i. d. R. dann in ein Archiv ausgelagert, wenn die Daten im Produktivbetrieb nicht länger benötigt werden, zur Gewährleistung gesetzlicher Vorgaben aber weiterhin gespeichert werden müssen. Ein Archiv ist also eher ein „Sammelbecken“ der unterschiedlichsten Daten und kann somit insbesondere Datenarten/-kategorien mit sehr unterschiedlichen Aufbewahrungsfristen und somit auch unterschiedlichen Löschvorgaben beinhalten. Daher ist es unabdingbar, dass in einem Archiv auch personenbezogene Daten gelöscht werden können.
   Grundsätzlich ist daher im Löschkonzept zu beschreiben, wie personenbezogene Daten in dem bzw. den jeweiligen Archiv(en) entsprechend den Vorgaben des Löschkonzeptes gelöscht werden.

b) Sicherungskopien, auch Backup genannt, dienen dazu, die Verfügbarkeit personenbezogener Daten sowie den Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Damit eine Wiederherstellung möglich ist, sollten Sicherungskopien vor Änderungen der Daten und insbesondere vor einem Löschen der Daten geschützt sein. Für Zwecke der Wiederherstellung benötigen Sicherungskopien jedoch nur relativ kurze Aufbewahrungszyklen; eine Wiederherstellung mit einem Backup, welches den Zeitpunkt von vor einem Jahr wiederherstellt, ist für medizinische Zwecke grundsätzlich ungeeignet und kann sogar Patientenleben gefährden, wenn für den betreffenden Patienten wichtige, aktuellere Daten nicht mehr verfügbar sind. Mit angemessenen kurzen Aufbewahrungsfristen für Backup-Generationen kann den rechtlichen Löschvorgaben jedoch genügt werden.
   Im Rahmen des Löschkonzeptes sind daher Löschfristen für die Backup-Generationen vorzusehen, welche einer zeitnahen Löschung von zu löschenden personenbezogenen Daten Rechnung tragen.

2.4.5 Überprüfung der Einhaltung des Löschkonzeptes

Um die Wirksamkeit wie auch die Einhaltung der im Löschkonzept vorgegebenen Regelungen sicherzustellen, muss die Einhaltung und Ausführung der Löschung regelmäßig überprüft werden. Hierzu muss im Löschkonzept festgehalten werden, wer dafür verantwortlich ist (siehe Abschnitt 2.4.1.4 auf Seite 30), daneben muss aber auch das Prüfintervall sowie das Verfahren zur

Prüfung und Dokumentation (was wird wie geprüft und wie wird die Prüfung dokumentiert) beschrieben sein.

2.4.6 Überprüfung/Anpassung der Vorgaben des Löschkonzeptes

In regelmäßigen Abständen muss das Löschkonzept – wie jedes andere Konzept auch – dahingehend überprüft werden, ob die Regelungen weiterhin den Anforderungen des Unternehmens entsprechen. Änderungen bzw. Anpassungen können z. B. erforderlich sein bei

- Änderungen der gesetzlichen Vorgaben:
  Gesetzesänderungen müssen rechtzeitig zum Wirkeintritt der regulatorischen Vorgaben eingepflegt werden. Daher ist ggf. auch eine zeitnahe Anpassung erforderlich. Fachgesetze werden i. d. R. von der jeweiligen Fachabteilung abgeglichen, dementsprechend sollte die Prüfung der Entwicklung der entsprechenden gesetzlichen Rahmenbedingungen auch bei der Fachseite liegen. Z. B.
    - Prüfung der Aufbewahrungsregelungen hinsichtlich Abrechnungsdaten bei der Verwaltung,
    - Prüfung der Aufbewahrungsvorgaben hinsichtlich der medizinischen Dokumentation bei der medizinischen Verwaltung, die für Ärzte, Pflegekräfte usw. verantwortlich ist (also Pflegedienstleitung und/oder ärztlicher Direktor) oder
    - Prüfung datenschutzrechtlicher Vorgaben beim Datenschutzbeauftragten.

  Es müssen jedoch Prozesse vorgesehen werden, wie, von wem und wann die Rückmeldungen in das Löschkonzept eingepflegt und wie die Änderungen im Unternehmen kommuniziert werden.
- Prozessänderungen im Unternehmen
  Prozessänderungen im Unternehmen sind im Gegensatz zu gesetzlichen Änderungen durch das Unternehmen selbst planbar. Jedoch müssen im Unternehmen Prozesse existieren, dass bei Änderungen Auswirkungen auf das Löschkonzept geprüft werden. Werden beispielsweise Abteilungen zusammengelegt, müssen ggf. nur die Verantwortlichkeiten bzgl. des Löschens geregelt werden, nicht jedoch die Vorgaben im Löschkonzept angepasst werden. Werden ggf. jedoch Kooperationen eingegangen, z. B. durch Erbringung von Dienstleistungen für andere Leistungserbringer wie beispielsweise Einbindung externer Labore, Teleradiologie usw., so sind ggf. neue Prozesse zu betrachten und im Löschkonzept zu integrieren.
- Änderungen der IT-Landschaft
  Änderungen in der IT-Landschaft haben i. d. R. keine grundlegenden Auswirkungen auf das Fachkonzept bzgl. des Vorgehens beim Löschen. Aber die Einführung neuer IT-Systeme bedingt beispielsweise Löschvorgaben für das System, da i. d. R. die Möglichkeiten, wie was gelöscht werden kann, von IT-System zu IT-System variieren. Das eine System kann jedes Datum einzeln löschen, andere nur komplette Datensätze, wieder andere nur zusammengehörende Fallakten. Auch Änderungen in der Organisationsstruktur können bedingen, dass Änderungen bzgl. Zuständigkeiten nachgepflegt werden müssen.

Es muss seitens des Unternehmens eine Person beauftragt werden, welchen den Prozess der Pflege des Löschkonzepts managt. Zu den Aufgaben dieser Person gehören insbesondere:

- Regelmäßig (zumindest jährlich) die Fachabteilungen aktiv bzgl. Änderungen der für sie geltenden Regelungen anzusprechen und zu vermerken, ob Änderungsbedarf besteht oder nicht
- In einem regelmäßigen Abstand (zumindest alle zwei bis drei Jahre) eine grundlegende Überprüfung des Löschkonzeptes zu initialisieren, in welcher nachvollzogen wird, ob das

Löschkonzept noch immer den Anforderungen des Unternehmens genügt und ob die beschriebenen Prozessabläufe vom Unternehmen weiterhin gelebt werden können.

2.5 Mitgeltende Unterlagen

- Datenschutzkonzept
- Rollen- und Berechtigungskonzept, beinhaltend die Festlegung der Rechte hinsichtlich des Löschens personenbezogener Daten
- Verfahrensverzeichnis der verantwortlichen Stelle bzw. Verzeichnis von Verarbeitungstätigkeiten
- Protokollierungskonzept
- Archivierungskonzept bzw. Archivordnung

2.6 Inkrafttreten

Dieses Löschkonzept tritt am Datum seiner Veröffentlichung in Kraft.

_____ _____

Datum der Veröffentlichung Unterschrift

2.7 Anlage: Rechtsgrundlagen und Aufbewahrungsfristen

Siehe Excel-Tabelle

aufbewahrungsfristen.xlsx

Teil III: Beispiele

1 Beispiel für eine Löschrichtlinie für in Dateisystemen/Ordnern unstrukturiert gespeicherten personenbezogenen Daten

Zur Erfüllung der dienstlichen Pflichten speichern Beschäftigte personenbezogene Daten u. a. in ihrem E-Mail-Postfach, aber auch im Dateisystem, sei es im eigenen Bereich oder in projekt- oder abteilungsbezogenen Ordnern. Diese unstrukturierte Datenspeicherung unterliegt denselben rechtlichen Regelungen wie die Speicherung personenbezogener Daten in Datenbanken, wie z. B. in unserem Krankenhausinformationssystem oder der von uns eingesetzten HR-Datenbank.

Für diese unstrukturiert gespeicherten Daten gelten die folgenden Regelungen:

1) Um eine angemessene Überprüfung bzgl. der Löschung unstrukturiert gespeicherter personenbezogener Daten zu gewährleisten, ist jede Abteilungsleitung verpflichtet, angemessene Verfahrensabläufe in schriftlicher Form festzulegen. Die einzelnen Abteilungen haben sich untereinander über die geeigneten Verfahrensabläufe abzustimmen. Diese Verfahrensanweisung muss insbesondere die folgenden Informationen beinhalten:
    a. Die gespeicherten personenbezogenen Daten
    b. Die Verarbeitungszwecke
    c. Die Aufbewahrungsfristen
    d. Für jede Kombination aus Verarbeitungszweck und Art der Daten sind die berechtigten Interessen und vertragliche oder rechtliche Pflichten zu ermitteln, die eine Verarbeitung bzw. Speicherung auch nach Ablauf einer rechtlichen Aufbewahrungsfrist erlauben bzw. erforderlich machen und – sofern vorhanden – in die Verfahrensanweisung aufzunehmen. Ggf. ist die Dauer, nach der ein berechtigtes Interesse hinfällig wird, samt Berechnungsmethode festzulegen und zu kommunizieren.
    e. Die Abstände, in welchen der Löschbedarf ermittelt werden muss. Bei der Festlegung der Überprüfungsabstände sind u. a. die folgenden Kriterien zu berücksichtigen:
        – Kosten,
        – Verarbeitungszweck und Sensibilität der personenbezogenen Daten.

        Ggf. sind für unterschiedliche Arten von Daten oder für unterschiedliche Verarbeitungszwecke individuelle Prüfrhythmen zu definieren. Eine Überprüfung ist mindestens einmal jährlich für sämtliche unstrukturiert gehaltenen personenbezogenen Daten durchzuführen; kürzere Intervalle sind möglich und ggf. notwendig.
    f. Die Zuständigkeit für die Überprüfung. Dies ist wie folgt zu regeln:
        – Für Daten, die nur einer Beschäftigten oder einem Beschäftigten persönlich zugänglich bzw. zugeordnet sind, führt jede bzw. jeder Beschäftigte die Überprüfung selbst durch. Dies betrifft insbesondere, aber nicht ausschließlich Nachrichten im eigenen E-Mail-Postfach, Dateien in lokalen Speichern auf dem persönlichen Arbeitsplatzrechner bzw. Mobilgerät, Dateien in den persönlichen Laufwerken im Firmennetz und Dateien auf mobilen Datenträgern, die einer Person direkt zugeordnet sind.
        – Für Daten, auf die mehrere Beschäftigte gemeinsam als Abteilung oder Team Zugriff haben, liegt die Zuständigkeit bei der Abteilungsleitung bzw. Teamleitung. Eine Unterdelegation auf einzelne Beschäftigte ist möglich; sie hat dann schriftlich zu erfolgen. Dies betrifft insbesondere, aber nicht ausschließlich Nachrichten in

gemeinsam genutzten E-Mail-Postfächern sowie Dateien in Abteilungslaufwerken im Firmennetz oder auf gemeinsam genutzten Datenträgern.

g. Das Verfahren bzgl. einer Freigabe der Löschung personenbezogener Daten. Hierbei sind folgende Vorgaben zu beachten:
   - Jede Abteilung und jede/-r Beschäftigte/r ist verpflichtet, regelmäßig die unstrukturiert gehaltenen personenbezogenen Daten in seinem/ihrem Verantwortungsbereich hinsichtlich der Notwendigkeit einer Löschung entsprechend der Verfahrensbeschreibung zu überprüfen.
   - Das Prüfergebnis wird dokumentiert und der Abteilungsleitung vorgelegt.
   - Die Abteilungsleitung entscheidet bzgl. der durchzuführenden Löschung. Die Entscheidung der Abteilungsleitung ist zu dokumentieren.

h. Die Art und Weise, wie die Löschung vorzunehmen ist. Dabei sind die Vorgaben aus dem Löschkonzept zu beachten.

i. Die Zuständigkeit für die Durchführung der Löschung. Bei der Festlegung der Zuständigkeit für die Durchführung der Löschung sind insbesondere die Fähigkeiten und Kenntnisse der Personen hinsichtlich des Umganges mit den zu diesem Vorgang gehörenden informationstechnischen Prozessen zu beachten. Ist in der eigenen Abteilung niemand mit den entsprechenden Kenntnissen vorhanden, so ist zu prüfen, welche/-r Beschäftigte/r die beste Eignung für eine entsprechende Weiterbildung aufweist. In Abhängigkeit auch von übergeordneten Compliance-Erwägungen und Geschäftsverteilungen kann die Zuständigkeit für die Durchführung des Löschens in der dienstleistenden IT-Abteilung oder auch in der Fachabteilung selbst liegen.

j. Der Umgang mit Daten, die trotz Löschpflicht nicht gelöscht werden. In diesen Fällen müssen die entgegenstehenden Gründe dokumentiert werden. Das voraussichtliche Löschdatum sollte – wenn möglich – angegeben werden. Dabei ist nicht zwingend eine exakte Datumsangabe erforderlich, z. B. „10 Jahre nach Entlassung des Patienten“ oder „nach dem nächsten Jahresabschluss“ ist möglich. Sofern eine Löschung noch nicht erfolgen darf, sind die personenbezogenen Daten bei der nächsten routinemäßigen Überprüfung erneut zu betrachten.

k. Eine Verpflichtung zur Protokollierung der Löschung entsprechend den Vorgaben im Löschkonzept.

2) Die Verfahrensanweisungen sind dem/der Datenschutzbeauftragten zur Freigabe vorzulegen und unmittelbar nach Freigabe anzuwenden.
3) Alle freigegebenen Verfahrensanweisungen zur Löschung unstrukturiert gespeicherter personenbezogener Daten werden leicht auffindbar und nachvollziehbar strukturiert im Intranet veröffentlicht.
4) Die Abteilungsleitung muss sicherstellen, dass alle im jeweiligen Bereich eingesetzten Beschäftigten über die Verfahrensanweisungen zur Löschung personenbezogener Daten informiert sind. Dies ist auch bei allen neu hinzukommenden Beschäftigten sicherzustellen.
5) Jede Abteilungsleitung hat Informationen über Ereignisse, die sich auf die Festlegung des Löschbedarfs auswirken können, an andere Abteilungen weiterzugeben, wenn davon auszugehen ist, dass andere Abteilungen personenbezogene Daten vorhalten, die von diesem Ereignis betroffen sein können. Ggf. ist eine vorübergehende Löschsperre auszusprechen.

2 Beispiel für ein Löschkonzept: IT-Dokumentationssystem für Brustkrebs

Im Krankenhaus „Gott-erbarme-dich“ wird das onkologische Informationssystem „DokuEasy“ zur Dokumentation der onkologischen Behandlung bei Brustkrebs innerhalb des von Onkozert zertifizierten Brustzentrums eingesetzt.

2.1 Geltungs- und Anwendungsbereich des Löschkonzeptes

Dieses Löschkonzept gilt für das Brustzentrum im Krankenhaus „Gott-erbarme-dich“ im Rahmen der Verarbeitung von Patientendaten durch das IT-System „DokuEasy“.

2.2 Definition von Datenarten/-kategorien und den für sie geltenden gesetzlichen Aufbewahrungsfristen

Es werden überwiegend Patientendaten verarbeitet, dabei beschränkt auf die Versorgung von an Brustkrebs erkrankten Patienten. Daneben werden Informationen von Beschäftigten verarbeitet, soweit diese für die Einhaltung der im Berechtigungskonzept beschriebenen Zugriffsrechte benötigt werden. Einzelheiten finden sich im Anhang 2.

2.3 Abwägung von Lösch- und Aufbewahrungsinteressen

Es erfolgt eine Löschung nach Ende der gesetzlich vorgeschriebenen Aufbewahrungsfristen.

Das Landeskrankenhausgesetz für das Land Inferno gestattet die Nutzung von Patientendaten zu Forschungszwecken. Gemäß Art. 5 Abs. 1 lit. e DS-GVO dürfen für wissenschaftliche Forschungszwecke Daten länger gespeichert werden. Die Datenverantwortliche kann für wissenschaftliche Forschungszwecke erforderliche Daten benennen, die dann länger gespeichert werden. In diesen Fällen muss in einer Liste festgehalten werden:

1) Der konkrete wissenschaftliche Forschungszweck
2) Der Nachweis der wissenschaftlichen Forschung[36]
3) Die Aufbewahrungsfrist, d. h. die konkrete Speicherdauer

2.4 Prozessbeschreibung

2.4.1 Festlegung der Verantwortlichkeiten

2.4.1.1 Geschäftsführung, welche die Gesamtverantwortung besitzt

Die Gesamtverantwortung für die Einhaltung gesetzlicher Vorgaben liegt in der Leitung des Krankenhauses „Gott-erbarme-dich“.

2.4.1.2 Datenverantwortliche, welche die Löschpflicht prüfen und falls erforderlich die Löschung anweisen

Zur Datenverantwortlichen, welche einerseits die Gültigkeit dieser Regelungen überwacht sowie bei evtl. auftretenden Fragestellungen die Entscheidung bzgl. Aufbewahren oder Löschen trifft, wurde die Leiterin unserer gynäkologischen Abteilung sowie des Brustzentrums benannt. Dies ist Frau Professor Polyhistor.

[36] Siehe hierzu auch: GMDS, GDD: Medizinische Forschung unter der DS-GVO, Kapitel 4.2. [Online] 2017 [Zitiert 2020-04-10] https://gesundheitsdatenschutz.org/html/forschung.php

2.4.1.3 Systemverantwortliche, welche die Löschung durchführen

Verantwortlich für die technische Umsetzung und Durchführung ist die IT-Abteilung unseres Krankenhauses „Gott-erbarme-dich“, namentlich in Person der Leitung der Abteilung 2, Herrn Claudius Augustus Moderatio.

2.4.1.4 Auditverantwortliche, welche die Einhaltung der Vorgaben prüfen

Durch die Qualitätsmanagement-Abteilung unseres Krankenhauses „Gott-erbarme-dich“ erfolgt eine Prüfung der Einhaltung dieser Regelungen im Rahmen der ISO 9001 Audits. Namentlich verantwortlich ist die derzeitige Leitung Schwester Inexorabilis vom Orden der fidelen Schwestern.

2.4.2 Umgang mit individuellen Löschanträgen durch betroffene Personen

Stellen Patienten oder ehemalige Patienten einen Antrag auf Löschung der sie betreffenden Daten, so wird diese Anfrage durch die Dokumentationsabteilung des Brustzentrums innerhalb der gesetzlich vorgesehenen Zeitspanne von maximal vier Wochen nach Antragseingang bearbeitet. Verantwortlich für die Einhaltung der Vorgaben ist die Leitung der Dokumentationsabteilung, Frau Marion Adjutor.

2.4.3 Einzuhaltende Vorgehensweisen bzw. Standards bei der Löschung insbesondere auch Protokollierung der Löschung

2.4.3.1 Löschzeiten

Die Löschzeiten ergeben sich unmittelbar aus der in Anhang 2 beschriebenen Aufbewahrungsfristen unter Berücksichtigung der in Abschnitt 2.3 genannten Einschränkungen.

2.4.3.2 Löschverfahren

Die Löschung erfolgt durch die vom IT-System „DokuEasy“ bereitgestellten Mechanismen, die laut Auskunft des Herstellers eine irreversible Datenvernichtung beinhalten.

2.4.3.3 Einschränkung der Verarbeitung („Sperrung)

Eine Sperrung erfolgt

1) Wie im Abschnitt 2.3 beschrieben
2) Wenn von der betroffenen Person die Richtigkeit der Daten bestritten wird, werden die Daten für die Dauer der Prüfung der Daten auf Richtigkeit gesperrt.
3) Erfolgte die Verarbeitung der Daten unrechtmäßig, werden die Daten gesperrt statt gelöscht, wenn die betroffene Person die Löschung ablehnt.
4) Daten werden gesperrt statt gelöscht, wenn der Verarbeitungszweck seitens unseres Krankenhauses erreicht ist und die Daten seitens des Verantwortlichen eigentlich zu löschen sind, die betroffene Person die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Dies kann z. B. für den Nachweis bzgl. anzurechnender Leistungen bzgl. Rente/Pension unserer Beschäftigten auf deren Antrag erfolgen.

Außerhalb der hier genannten Fälle erfolgt eine Sperrung statt Löschung nur im Rahmen gesetzlicher Verpflichtungen, wenn beispielsweise im Verlauf eines Rechtsstreites eine gerichtliche Anordnung die Löschung verbietet oder Daten in Gerichtsverfahren verwendet werden müssen, sodass eine Löschung nicht erfolgen darf.

2.4.3.4 Löschprotokoll

Jede Löschung wird protokolliert. Im Löschprotokoll sind folgende Inhalte enthalten:

- Datenverantwortliche Stelle (also z. B. Personalabteilung oder Gynäkologie)
- Datum und Uhrzeit der Löschung
- Für die Löschung verantwortliche Person, d. h. die/der Datenverantwortliche (inkl. Rolle/Funktionen)
- Die ausführenden Personen (inkl. Rollen/Funktionen)
- Die Methode der Datenlöschung
- Eine Beschreibung der zu löschenden Daten, Datenarten/-kategorien
- Die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport); wurden Daten an Dritte weitergegeben ggf. entsprechendes Aktenzeichen zur Abarbeitung von Nachfragen dokumentieren, wenn gewährleistet ist, dass damit keine Person identifiziert, sondern nur die Löschung beauskunftet werden kann
- Die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport)

2.4.4 Umgang mit Archiven sowie Sicherungskopien

Die Archivierung der Patientendaten erfolgt innerhalb des IT-Systems „DokuEasy“, d. h. außerhalb dieses IT-Systems werden seitens des Brustzentrums keine Daten zu Zwecken der Langzeitarchivierung gespeichert.

Wie im Backupkonzept unseres Krankenhauses beschrieben ist, erfolgt eine Sicherung unserer Daten im sogenannten „Generationenprinzip“. Jede Nacht wird ein Backup der Daten angelegt:

- An jedem ersten Dienstag im Monat wird ein vollständiges Backup angelegt, welches alle sechs Monate überschrieben wird.
- Jeden Montag wird ein vollständiges Backup angelegt, welches jede zweite Woche überschrieben wird.
- Dienstag bis Sonntag wird täglich ein inkrementelles Backup angelegt, d. h. es werden nur die seit dem letzten Backup geänderten oder neu hinzugekommenen Daten gesichert. Diese Sicherungsdaten werden jede Woche überschrieben.

D. h. im Rahmen der Datensicherung werden Daten spätestens alle 6 Monate gelöscht.

2.4.5 Überprüfung der Einhaltung des Löschkonzeptes

Eine Prüfung der Einhaltung dieser Regelungen durch die Qualitätsmanagement-Abteilung erfolgt im Rahmen der jährlich stattfinden ISO 9001 Audits.

Zusätzlich erfolgt bei Feststellung von Abweichungen zum Zeitpunkt dieser Feststellung eine Überprüfung durch den Datenschutzbeauftragten unseres Krankenhauses.

2.4.6 Überprüfung/Anpassung der Vorgaben des Löschkonzeptes

Die Datenverantwortliche des Brustzentrums prüft alle zwei Jahre, ob die Inhalte dieses Löschkonzeptes

1) den gesetzlichen Erfordernissen entsprechen,
2) die Prozesse innerhalb unseres Krankenhauses den gesetzlichen Anforderungen genügen

und wird bei Bedarf Änderungen an diesem Löschkonzept veranlassen. Alle erforderlichen Fachabteilungen wie beispielsweise IT-Abteilung oder Rechtsabteilung haben die Datenverantwortliche hierbei vollumfänglich zu unterstützen.

2.5 Mitgeltende Unterlagen

- Datenschutzkonzept
- Rollen- und Berechtigungskonzept
- Verzeichnis von Verarbeitungstätigkeiten
- Protokollierungskonzept
- Archivordnung

2.6 Inkrafttreten

Dieses Löschkonzept tritt am Datum seiner Veröffentlichung in Kraft.

Datum der Veröffentlichung: 1. April 2020

Unterschrift: xXx (Geschäftsführer)

2.7 Anhang 1: Rechtsgrundlagen und Aufbewahrungsfristen

An dieser Stelle werden die Regelwerke lediglich benannt, die Zuordnung zu den jeweiligen Abschnitten der Regelwerke, wie beispielsweise Paragraphen, erfolgt in Anhang 2. Diese Liste dient in erster Linie der Übersicht, welche gesetzlichen Rahmenbedingungen zu beachten sind, aber auch der Darstellung der in Anhang 2 verwendeten Abkürzungen der Regelwerke. Die Benennung der Regelungen erfolgt in alphabetischer Reihenfolge:

1) Berufsordnung für die Ärztinnen und Ärzte des Bundeslandes Inferno
2) Bürgerliches Gesetzbuch (BGB)
3) Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen (GCP-V)

2.8 Anhang 2: Zuordnung Datenarten und Aufbewahrungsfrist

Nr.	Datenart/-kategorie	Personengruppe	Verwendungszweck	Aufbewahrungsfrist	Rechtsgrundlage
1	Stammdaten	Patienten	Identifikation, Zuordnung Daten	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
2	Stammdaten	Beschäftigte	Identifikation / Anmeldung System	2 Jahre nach Ausscheiden	Zugriffssteuerung im IT-System; Beauskunftung betr. Personen bzgl. Zugriff
3	Löschprotokolle	Beschäftigte	Nachweis der Löschung pbD	Bis zum Ende des auf der Generierung folgenden Jahres	Keine
4	Anamnesen	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
5	Untersuchungen sowie Ergebnisse	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
6	Scorewerte, Klassifikationen usw.	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
7	Therapien	Patienten	Med. Dokumentation	10 Jahre nach Abschluss	§ 630f BGB § 10 Abs. 3 BO-Ä

				Behandlung	
8	Komplikationen	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
9	Nachsorge	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä

Hinweise / zu beachtende Rahmenbedingungen:

- Chemotherapeutika werden in der Apotheke hergestellt, daher werden evtl. zu beachtende Aufbewahrungsfristen bzgl. der Herstellung der Chemotherapeutika dort umgesetzt. In „DokuEasy“ wird lediglich die Anwendung der Chemotherapie selbst dokumentiert, bzgl. Aufbewahrungsfristen gelten hier nur die Vorgaben, welche auch für alle anderen medizinischen Dokumentationsprozesse gelten.
- Strahlentherapien werden von der Abteilung für Strahlentherapie geplant und durchgeführt, evtl. in dieser Hinsicht zu beachtende Aufbewahrungsfristen werden dort umgesetzt. In „DokuEasy“ wird lediglich die Durchführung einer Strahlentherapie dokumentiert, bzgl. Aufbewahrungsfristen gelten hier nur die Vorgaben, welche auch für alle anderen medizinischen Dokumentationsprozesse gelten.
- Radiologische Untersuchungen wie MRT oder CT werden von der Radiologie durchgeführt, evtl. in dieser Hinsicht zu beachtende Aufbewahrungsfristen werden dort umgesetzt. In „DokuEasy“ wird nur die Durchführung der Untersuchung selbst sowie die Ergebnisse der Untersuchung dokumentiert, bzgl. Aufbewahrungsfristen gelten hier nur die Vorgaben, welche auch für alle anderen medizinischen Dokumentationsprozesse gelten.
- Eine Aufbewahrung nach Abschluss der Behandlung dient in erster Linie therapeutischen Belangen. In der Gesetzesbegründung zum Patientenrechtegesetz findet sich, dass die Pflicht zur Aufbewahrung im Einzelfall weit über zehn Jahre hinausgehen kann, wenn es z. B. der gesundheitliche Zustand des Patienten erfordert[37]. Die Behandlung von Brustkrebs ist i. d. R. niemals vollkommen abgeschlossen, da Krebszellen regelhaft im Körper verbleiben und ein Rezidiv auslösen können, weswegen regelhaft Nachsorgeuntersuchungen angesetzt werden um den Verlauf der Erkrankung unter ärztlicher Beobachtung zu behalten. § 630f BGB schreibt, analog zu § 10 Abs. 3 MBO-Ä, eine Aufbewahrung der Patientenakte „für die Dauer von zehn Jahren nach Abschluss der Behandlung“ vor. D. h. die Aufbewahrungsdauer endet erst zehn Jahre nach Abschluss der Behandlung. In zu begründeten Einzelfällen kann daher ggf. gerade bei Patienten mit Brustkrebs der gesetzliche Aufbewahrungszeitraum von 10 Jahren erst entsprechend lange nach dem letzten Kontakt mit dem Patienten beginnen und dementsprechend lange müssen Daten ggf. aufbewahrt werden, ggf. endet die Aufbewahrungsfrist erst mit bzw. nach dem Tod des Patienten.

2.9 Anhang 3: Angaben zu wissenschaftlichen Forschungszwecken, welche eine längere Aufbewahrungsfrist erfordern

1) Beobachtungsstudie bzgl. taxanhaltiger Medikamente

[37] Bundesregierung, BT-Drs. 17/10488: Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten. Seite 26, 2. Spalte 3. Absatz. [Online] 2013 [Zitiert 2020-04-10] http://dip21.bundestag.de/dip21/btd/17/104/1710488.pdf

Zu den Standardtherapien bei Brustkrebs zählen taxanhaltige Medikamente wie Docetaxel oder auch Paclitaxel. In dieser Studie sollen die Medikamente auf ihre Wirkung und Verträglichkeit untersucht werden.

a. Benötigte Daten: Daten sowohl von Patienten, die mit diesen Medikamenten behandelt wurden, als auch Daten von Patienten, wo diese Medikamente nicht angewendet wurden (Vergleichsgruppe); an Daten werden benötigt (näheres siehe Studienprotokoll): Patientenstammdaten, Klassifikation der Erkrankung, Diagnosen inkl. Begleiterkrankungen, durchgeführte Therapien, Komplikationen, Daten der Nachsorge
b. Nachweis „Wissenschaftliche Forschung“
   Entsprechend der Definition im Papier[38] von GMDS und GDD ist Forschung „die systematische Suche nach neuen Erkenntnissen sowie deren Dokumentation und Veröffentlichung, wobei Suche sowohl im Bereich der Grundlagenforschung als auch der angewandten Forschung erfolgen kann“, wobei „Wissenschaft“ verlangt, dass ein „ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit“ vorgenommen wird.
   Die Studie ist eine Beobachtungsstudie, bei der vor Beginn der Studie
   - Fragestellung,
   - Einschlusskriterien,
   - Vorgehensweise während der Studie,
   - Auswertung und
   - Veröffentlichung der Ergebnisse

   in einem Studienplan festgelegt wurden. Es handelt sich bei der Studie also um einen „ernsthaften, planmäßigen Versuch“.
   Entsprechend ErwGr. 159 DS-GVO zählen Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden, zur Forschung. Brustkrebs ist eine der am häufigsten auftretenden Krebsarten, bei welcher Befragungen immer ergaben, dass ein deutliches Interesse der Öffentlichkeit an einer Optimierung der Therapie besteht. Laut ErwGr. 156 DS-GVO zählen ebenso klinische Prüfungen, wie sie in dieser Beobachtungsstudie erfolgt, ebenfalls zur Forschung. Und laut ErwGr. 157 DS-GVO zählen Untersuchungen, welche eine Verbesserung der Lebensqualität zahlreicher Menschen ergeben können, ebenfalls zur Forschung i. S. d. DS-GVO.
   Die vorliegende Beobachtungsstudie stellt als eine wissenschaftliche Forschung dar.
c. Aufbewahrungsfrist: 10 Jahre nach Studienende zum Nachweis der Studienergebnisse; nach Studienende werden die Daten anonymisiert, falls gesetzliche Aufbewahrungsvorgaben überschritten wurden.

2) Usw.

[38] : GMDS, GDD: Medizinische Forschung unter der DS-GVO, Kapitel 4.1 und 4.2. [Online] 2017 [Zitiert 2020-04-10] https://gesundheitsdatenschutz.org/html/forschung.php

3 Beispiel für ein Löschkonzept: Personalverwaltung mit SAP

SAP wird insbesondere in größeren Organisationen häufig zur Personalverwaltung eingesetzt. SAP führte das „Information Lifecycle Management“ (ILM) ein[39], welches ermöglicht

- Bedingungsfelder, von welchen Aufbewahrungsdauern abhängen, zu nutzen sowie
- Startzeitpunkte festzulegen, ab denen Aufbewahrungsdauern gelten.

Bei der Datenarchivierung werden diese Regelwerke interpretiert und aus der Ableitung dieser Aufbewahrungsregelungen die Aufbewahrungsdauer ermittelt; die Pflege der Regelwerke und Regeln erfolgt über die Anwendung mit dem Information Retention Manager (IRM) über die Transaktion IRMPOL. Die Datenvernichtung selbst erfolgt mit Hilfe von Archivierungsobjekten.

Wenn ohne Archivierungsfunktion gearbeitet werden soll, können ILM-Objekte zu sogenannten „Datenvernichtungsobjekten“ erweitert werden; eine Löschung von Daten ist auch unter diesen Umständen möglich; die Pflege erfolgt über die Transaktion DOBJ.

Die Voraussetzung zur Nutzung der Löschfunktion in SAP Human Capital Management (HCM): es muss mindestens SAP ERP 6.0 mit Enhancement Package (EHP) 6.0 support package stack (SPS) 16 vorhanden sein; die Nutzung von ILM ist lizenzpflichtig, jedoch ist die Lizenz für ILM in HCM enthalten, wenn ILM nur für die Datenvernichtung genutzt wird.

3.1 Geltungs- und Anwendungsbereich des Löschkonzeptes

Dieses Löschkonzept gilt für die Personalverwaltung im Krankenhaus „Gott-erbarme-dich“. Alle Personaldaten werden in SAP HCM verarbeitet. Werden Daten wie beispielsweise die monatliche Gehaltsliste an die Beschäftigte selbst übergeben, so sind für diese Daten die Beschäftigten selbst verantwortlich im datenschutzrechtlichen Sinne, d. h. diese Regelungen finden für die den Betroffenen übergebenen Daten keine Anwendung.

3.2 Definition von Datenarten/-kategorien und den für sie geltenden gesetzlichen Aufbewahrungsfristen

Die Datenerfassung in SAP HCM erfolgt in Infotypen. Infotypen sind Datensätze, welche mehrere inhaltlich zusammenhängende Informationen verarbeiten. Der Infotyp 0009[40] „Bankverbindung“ beinhaltet daher z. B. neben dem Namen der Bank auch Angaben zur International Bank Account Number (IBAN). Für jeden Infotypen muss daher die für sie geltenden Aufbewahrungsfristen festgelegt werden. Diese Festlegung erfolgte in Anhang 2.

3.3 Abwägung von Lösch- und Aufbewahrungsinteressen

Es erfolgt eine Löschung nach Ende der gesetzlich vorgeschriebenen Aufbewahrungsfristen. Bedingt durch die Vorgaben innerhalb SAP erfolgt der Beginn der Zeitrechnung bzgl. der Aufbewahrungsfrist mit Erreichen des Jahresendes nach Anlage, sodass ggf. Daten bis zu einem Jahr länger gespeichert werden. In diesen Fällen erfolgt eine Sperrung der Daten, sodass diese Daten – abgesehen von der Speicherung – nicht länger durch unser Krankenhaus resp. durch Beschäftigte des Krankenhauses verarbeitet werden können.

---

[39] SAP Dokumentation: Datenvernichtung im HR. [Online] 2013 [Zitiert 2020-04-10]´ https://help.sap.com/doc/erp_hcm_ias_2013_01/1.0.3/de-DE/12/3ec27674e845e98c137358014f1aa7/frameset.htm

[40] SAP Dokumentation: Bankverbindung (Infotyp 0009). [Online] 2013 [Zitiert 2020-04-10] https://help.sap.com/erp_hcm_ias2_2015_02/helpdata/de/00/9257181bab43df8a4ec81aaef2364b/frameset.htm

3.4 Prozessbeschreibung

3.4.1 Festlegung der Verantwortlichkeiten

3.4.1.1 Geschäftsführung, welche die Gesamtverantwortung besitzt

Die Gesamtverantwortung für die Einhaltung gesetzlicher Vorgaben liegt in der Leitung unseres Krankenhauses „Gott-erbarme-dich“.

3.4.1.2 Datenverantwortliche, welche die Löschpflicht prüfen und falls erforderlich die Löschung anweisen

Zum Datenverantwortlichen, welche einerseits die Gültigkeit dieser Regelungen überwacht sowie bei evtl. auftretenden Fragestellungen die Entscheidung bzgl. Aufbewahren oder Löschen trifft, wurde Schwester Crudelis vom Orden der fidelen Schwestern benannt.

3.4.1.3 Systemverantwortliche, welche die Löschung durchführen

Verantwortlich für die technische Umsetzung und Durchführung ist die IT-Abteilung unseres Krankenhauses „Gott-erbarme-dich“, namentlich in Person der Leitung der Abteilung 2, Frau Marion Stornix.

3.4.1.4 Auditverantwortliche, welche die Einhaltung der Vorgaben prüfen

Durch die Controlling-Abteilung unseres Krankenhauses „Gott-erbarme-dich“ erfolgt eine Prüfung der Einhaltung dieser Regelungen. Namentlich verantwortlich ist die derzeitige Leitung Herr Thomas Gnadenlos.

3.4.2 Umgang mit individuellen Löschanträgen durch betroffene Personen

Stellen Beschäftigte oder ehemalige Beschäftigte einen Antrag auf Löschung der sie betreffenden Daten, so wird diese Anfrage durch die Personalverwaltung innerhalb der gesetzlich vorgesehenen Zeitspanne von maximal vier Wochen nach Antragseingang bearbeitet.

3.4.3 Einzuhaltende Vorgehensweisen bzw. Standards bei der Löschung insbesondere auch Protokollierung der Löschung

3.4.3.1 Löschzeiten

Die Löschzeiten ergeben sich unmittelbar aus den in Anhang 2 beschriebenen Aufbewahrungsfristen unter Berücksichtigung der in Abschnitt 3.3 genannten Einschränkungen.

3.4.3.2 Löschverfahren

Die Löschung erfolgt durch die in SAP HCM bereitgestellten Mechanismen, die laut Auskunft des Herstellers eine irreversible Datenvernichtung beinhalten[41].

3.4.3.3 Einschränkung der Verarbeitung („Sperrung)

Eine Sperrung erfolgt

1) Wie im Abschnitt 3.3 beschrieben
2) Wenn von der betroffenen Person die Richtigkeit der Daten bestritten wird, werden die Daten für die Dauer der Prüfung der Daten auf Richtigkeit gesperrt.
3) Erfolgte die Verarbeitung der Daten unrechtmäßig, werden die Daten gesperrt statt gelöscht, wenn die betroffene Person die Löschung ablehnt.

[41] SAP Dokumentation: Datenvernichtung im HR. [Online] 2013 [Zitiert 2020-04-10]´ https://help.sap.com/doc/erp_hcm_ias_2013_01/1.0.3/de-DE/12/3ec27674e845e98c137358014f1aa7/frameset.htm

4) Daten werden gesperrt statt gelöscht, wenn der Verarbeitungszweck seitens unseres Krankenhauses erreicht ist und die Daten seitens des Verantwortlichen eigentlich zu löschen sind, die betroffene Person die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Dies kann z. B. für den Nachweis bzgl. anzurechnender Leistungen bzgl. Rente/Pension unserer Beschäftigten auf deren Antrag erfolgen.

Außerhalb der hier genannten Fälle erfolgt eine Sperrung statt Löschung nur im Rahmen gesetzlicher Verpflichtungen, wenn beispielsweise im Verlauf eines Rechtsstreites eine gerichtliche Anordnung die Löschung verbietet oder Daten in Gerichtsverfahren verwendet werden müssen, sodass eine Löschung nicht erfolgen darf.

3.4.3.4 Löschprotokoll

Jede Löschung wird protokolliert. Im Löschprotokoll sind folgende Inhalte enthalten:

- Datenverantwortliche Stelle (also z. B. Personalabteilung oder Gynäkologie)
- Datum und Uhrzeit der Löschung
- Für die Löschung verantwortliche Person, d. h. die/der Datenverantwortliche (inkl. Rolle/Funktionen)
- Die ausführenden Personen (inkl. Rollen/Funktionen)
- Die Methode der Datenlöschung
- Eine Beschreibung der zu löschenden Daten, Datenarten/-kategorien
- Die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport); wurden Daten an Dritte weitergegeben ggf. entsprechendes Aktenzeichen zur Abarbeitung von Nachfragen dokumentieren, wenn gewährleistet ist, dass damit keine Person identifiziert, sondern nur die Löschung beauskunftet werden kann
- Die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport)

3.4.4 Umgang mit Archiven sowie Sicherungskopien

Die Archivierung der Personaldaten erfolgt innerhalb von HCM, d. h. außerhalb von HCM werden zu Zwecken der Langzeitarchivierung keine Daten gespeichert.

Wie im Backupkonzept unseres Krankenhauses beschrieben ist, erfolgt eine Sicherung unserer Daten im sogenannten „Generationenprinzip“. Jede Nacht wird ein Backup der Daten angelegt:

- An jedem ersten Dienstag im Monat wird ein vollständiges Backup angelegt, welches alle sechs Monate überschrieben wird.
- Jeden Montag wird ein vollständiges Backup angelegt, welches jede zweite Woche überschrieben wird.
- Dienstag bis Sonntag wird täglich ein inkrementelles Backup angelegt, d. h. es werden nur die seit dem letzten Backup geänderten oder neu hinzugekommenen Daten gesichert. Diese Sicherungsdaten werden jede Woche überschrieben.

D. h. im Rahmen der Datensicherung werden Daten spätestens alle 6 Monate gelöscht.

3.4.5 Überprüfung der Einhaltung des Löschkonzeptes

Eine Prüfung der Einhaltung dieser Regelungen durch die Controlling-Abteilung erfolgt im Abstand von zwei Jahren.

Zusätzlich erfolgt bei Feststellung von Abweichungen zum Zeitpunkt dieser Feststellung eine Überprüfung.

3.4.6 Überprüfung/Anpassung der Vorgaben des Löschkonzeptes

Die Datenverantwortliche für den Bereich Personaldatenverarbeitung prüft alle zwei Jahre, ob die Inhalte dieses Löschkonzeptes

3) den gesetzlichen Erfordernissen entsprechen,
4) die Prozesse innerhalb unseres Krankenhauses den gesetzlichen Anforderungen genügen

und wird bei Bedarf Änderungen an diesem Löschkonzept veranlassen. Alle erforderlichen Fachabteilungen wie beispielsweise IT-Abteilung oder Rechtsabteilung haben die Datenverantwortliche hierbei vollumfänglich zu unterstützen.

3.5 Mitgeltende Unterlagen

- Datenschutzkonzept
- Rollen- und Berechtigungskonzept
- Verzeichnis von Verarbeitungstätigkeiten
- Protokollierungskonzept
- Archivordnung

3.6 Inkrafttreten

Dieses Löschkonzept tritt am Datum seiner Veröffentlichung in Kraft.

Datum der Veröffentlichung: 1. April 2018

Unterschrift: xXx (Geschäftsführer)

3.7 Anhang 1: Rechtsgrundlagen und Aufbewahrungsfristen

An dieser Stelle werden die Regelwerke lediglich benannt, die Zuordnung zu den jeweiligen Abschnitten der Regelwerke, wie beispielsweise Paragraphen, erfolgt in Anhang 2. Diese Liste dient in erster Linie der Übersicht, welche gesetzlichen Rahmenbedingungen zu beachten sind, aber auch der Darstellung der in Anhang 2 verwendeten Abkürzungen der Regelwerke. Die Benennung der Regelungen erfolgt in alphabetischer Reihenfolge:

1) Abgabenordnung (AO)
2) Allgemeines Gleichbehandlungsgesetz (AGG)
3) Arbeitszeitgesetz (ArbZG)
4) Drittes Buch Sozialgesetzbuch – Arbeitsförderung (SGB III)
5) Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (GwG)
6) Gesetz über den Wertpapierhandel (WpHG)
7) Gesetz zum Schutz von Müttern bei der Arbeit, in der Ausbildung und im Studium (MuSchG)
8) Gesetz zum Schutze der arbeitenden Jugend (JArbSchG)
9) Handelsgesetzbuch (HGB)
10) Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung (SGB VII)
11) Umsatzsteuergesetz (UStG)
12) Verordnung über die Rechnungs- und Buchführungspflichten von Krankenhäusern (KHBV)

13) Verordnung über Sicherheit und Gesundheitsschutz bei Tätigkeiten mit Biologischen Arbeitsstoffen (BioStoffV
14) Verordnung zum Schutz vor Gefahrstoffen (GefStoffV)
15) Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV)
16) Viertes Buch Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung (SGB IV)

3.8 Anhang 2: Zuordnung Infotypen und Aufbewahrungsfrist

Infotyp-Nr.	Infotyp-Bezeichnung	Personengruppe	Verwendungszweck	Aufbewahrungsfrist	Rechtsgrundlage
0000	Maßnahmen	Beschäftigte			
0001	Organisatorische Zuordnung	Beschäftigte			
…					

4 Beispiel für ein Löschkonzept: Arztpraxis für Allgemeinmedizin

Die Praxis für Allgemeinmedizin wird von den zwei Fachärzten, den Dres. Hermine und Harald Sanarius geführt. Die Ärzte setzen in ihrer Praxis das Praxisverwaltungssystem (PVS) „Schreib es auf“ ein, außerhalb des PVS werden keine Patientendaten langfristig gespeichert.

Den kompletten Bereich der Verwaltung ihrer Beschäftigtendaten inkl. der Lohnbuchhaltung wurde an die Firma DAVO übergeben, welche diesen Bereich der Datenverarbeitung eigenverantwortlich inkl. regelhafter Löschung der Daten führt.

Für kleine Arztpraxen bis zu 20 Beschäftigten besteht keine Benennpflicht für einen internen oder externen Datenschutzbeauftragten. Aber die DS-GVO legt diesen Praxen vielfältige Pflichten im Rahmen von Dokumentationen, Nachweisen und Belehrungen der Beschäftigten usw. auf. Eine Rechtsberatung durch Anwälte kann dabei manchmal sehr teuer werden, andererseits gibt es immer wieder Datenschutzfragen. Daher kann es auch für kleine Praxen aus betriebswirtschaftlicher Sichtweise angezeigt sein, auch ohne gesetzliche Verpflichtung einen Datenschutzbeauftragen zu benennen.

4.1 Geltungs- und Anwendungsbereich des Löschkonzeptes

Dieses Löschkonzept gilt für die Speicherung von Patientendaten in der Praxis Dres. Sanarius

4.2 Definition von Datenarten/-kategorien und den für sie geltenden gesetzlichen Aufbewahrungsfristen

Es werden überwiegend Patientendaten verarbeitet. Informationen von Beschäftigten werden nur verarbeitet, soweit diese Verarbeitung für die Prüfung und Umsetzung von Zugriffsrechten auf Patientendaten erforderlich sind. Einzelheiten finden sich im Anhang 2.

4.3 Abwägung von Lösch- und Aufbewahrungsinteressen

Es erfolgt eine Löschung nach Ende der gesetzlich vorgeschriebenen Aufbewahrungsfristen (siehe Anhang 2).

4.4 Prozessbeschreibung

4.4.1 Festlegung der Verantwortlichkeiten

1) Gesamtverantwortung: Die Gesamtverantwortung für die Einhaltung gesetzlicher Vorgaben liegt in der Leitung Arztpraxis.
2) Prüfung Einhaltung des Konzepts, Richtigkeit des Konzepts: Frau Dr. Sanatorius
3) Auditierung: Frau Dr. Sanatorius
4) Technische Umsetzung: Herr Max Meier, Geschäftsführer der Firma Medfactio
5) Auftragsverarbeiter ist die Firma Medfactio, welche das eingesetzte PVS auch herstellen und warten

4.4.2 Umgang mit individuellen Löschanträgen durch betroffene Personen

Stellen Patienten oder ehemalige Patienten einen Antrag auf Löschung der sie betreffenden Daten, so wird dieser Anfrage durch Frau Dr. Sanatorius innerhalb der gesetzlich vorgesehenen Zeitspanne von maximal vier Wochen nach Antragseingang bearbeitet.

4.4.3 Einzuhaltende Vorgehensweisen bzw. Standards bei der Löschung insbesondere auch Protokollierung der Löschung

4.4.3.1 Löschzeiten

Die Löschzeiten ergeben sich unmittelbar aus der in Anhang 2 beschriebenen Aufbewahrungsfristen unter Berücksichtigung der in Abschnitt 2.3 Einschränkungen.

4.4.3.2 Löschverfahren

Die Löschung erfolgt durch die vom IT-System „Schreib es auf“ bereitgestellten Mechanismen, die laut Auskunft des Herstellers eine irreversible Datenvernichtung beinhalten.

4.4.3.3 Einschränkung der Verarbeitung („Sperrung)

Eine Sperrung erfolgt

1) Wenn von der betroffenen Person die Richtigkeit der Daten bestritten wird, werden die Daten für die Dauer der Prüfung der Daten auf Richtigkeit gesperrt.
2) Erfolgte die Verarbeitung der Daten unrechtmäßig, werden die Daten gesperrt statt gelöscht, wenn die betroffene Person die Löschung ablehnt.
3) Daten werden gesperrt statt gelöscht, wenn der Verarbeitungszweck seitens unserer Arztpraxis erreicht ist und die Daten eigentlich zu löschen sind, die betroffene Person die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.

Außerhalb der hier genannten Fälle erfolgt eine Sperrung statt Löschung nur im Rahmen gesetzlicher Verpflichtungen, wenn beispielsweise im Verlauf eines Rechtsstreites eine gerichtliche Anordnung die Löschung verbietet oder Daten in Gerichtsverfahren verwendet werden müssen, sodass eine Löschung nicht erfolgen darf.

4.4.3.4 Löschprotokoll

Jede Löschung wird durch den Auftragsverarbeiter protokolliert. Im Löschprotokoll sind folgende Inhalte enthalten:

- Datenverantwortliche Stelle (also z. B. Personalabteilung oder Gynäkologie)
- Datum und Uhrzeit der Löschung
- Für die Löschung verantwortliche Person, d. h. die/der Datenverantwortliche (inkl. Rolle/Funktionen)
- Die ausführenden Personen (inkl. Rollen/Funktionen)
- Die Methode der Datenlöschung
- Eine Beschreibung der zu löschenden Daten, Datenarten/-kategorien
- Die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport); wurden Daten an Dritte weitergegeben ggf. entsprechendes Aktenzeichen zur Abarbeitung von Nachfragen dokumentieren, wenn gewährleistet ist, dass damit keine Person identifiziert, sondern nur die Löschung beauskunftet werden kann
- Die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport)

4.4.4 Umgang mit Archiven sowie Sicherungskopien

Die Archivierung der Patientendaten erfolgt innerhalb des IT-Systems „Schreib es auf“, eine weitere Langzeitarchivierung erfolgt nicht.

Wie im Backupkonzept beschrieben ist, erfolgt eine Sicherung unserer Daten im sogenannten „Generationenprinzip“. Jede Nacht wird ein Backup der Daten angelegt:

- An jedem ersten Dienstag im Monat wird ein vollständiges Backup angelegt, welches alle sechs Monate überschrieben wird.
- Jeden Montag wird ein vollständiges Backup angelegt, welches jede zweite Woche überschrieben wird.
- Dienstag bis Sonntag wird täglich ein inkrementelles Backup angelegt, d. h. es werden nur die seit dem letzten Backup geänderten oder neu hinzugekommenen Daten gesichert. Diese Sicherungsdaten werden jede Woche überschrieben.

D. h. im Rahmen der Datensicherung werden Daten spätestens alle 6 Monate gelöscht.

4.4.5 Überprüfung der Einhaltung des Löschkonzeptes sowie Anpassungsbedarf

Frau Dr. Hermine Sanarius prüft alle zwei Jahre die Einhaltung dieser Regelungen in Form eines Audits und protokolliert die Auditergebnisse. Desgleichen prüft sie alle zwei Jahre, ob die Inhalte dieses Löschkonzeptes

1) den gesetzlichen Erfordernissen entsprechen und
2) die Prozesse innerhalb der Arztpraxis den gesetzlichen Anforderungen genügen

und wird bei Bedarf Änderungen an diesem Löschkonzept veranlassen.

4.5 Inkrafttreten

Dieses Löschkonzept tritt am Datum seiner Veröffentlichung in Kraft.

Datum der Veröffentlichung: 1. April 2018

Unterschrift: xYx (Dr. Hermine Sanatorius) xXx (Dr. Harald Sanarius)

4.6 Anhang 1: Rechtsgrundlagen und Aufbewahrungsfristen

An dieser Stelle werden die Regelwerke lediglich benannt, die Zuordnung zu den jeweiligen Abschnitten der Regelwerke, wie beispielsweise Paragraphen, erfolgt in Anhang 2. Diese Liste dient in erster Linie der Übersicht, welche gesetzlichen Rahmenbedingungen zu beachten sind, aber auch der Darstellung der in Anhang 2 verwendeten Abkürzungen der Regelwerke. Die Benennung der Regelungen erfolgt in alphabetischer Reihenfolge:

4) Berufsordnung für die Ärztinnen und Ärzte des Bundeslandes Inferno
5) Bürgerliches Gesetzbuch (BGB)
6) Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen (GCP-V)

4.7 Anhang 2: Zuordnung Datenarten und Aufbewahrungsfrist

Nr.	Datenart/-kategorie	Personengruppe	Verwendungszweck	Aufbewahrungsfrist, Löschzeitpunkt	Rechtsgrundlage
1	Stammdaten	Patienten	Identifikation, Zuordnung Daten	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä
2	Stammdaten	Beschäftigte	Identifikation / Anmeldung System	2 Jahre nach Ausscheiden	– Art. 15 DS-GVO (Beauskunftung betr. Personen bzgl. Zugriff) – Art, 32 Abs. 1lit. b DS-GVO (Gewährleistung der Vertraulichkeit durch Zugriffssteuerung im IT-System)
3	Löschprotokolle	Beschäftigte, Auftragsverarbeiter	Nachweis der Löschung pbD	Bis zum Ende des auf der Generierung folgenden Jahres	Keine
4	Medizinische Daten (Anamnesen, Diagnosen, Therapien, usw.)	Patienten	Med. Dokumentation	10 Jahre nach Abschluss Behandlung	§ 630f BGB § 10 Abs. 3 BO-Ä