



## SACHSEN-ANHALT

Landesbeauftragter  
für den Datenschutz

# Datenschutzgerechtes Vernichten von Gesundheitsdaten

Alle personenbezogenen Daten von Patientinnen und Patienten sind unabhängig von Ihrer Speicherart (z. B. elektronisch oder in Papierform) nach einem bestimmten Zeitablauf zu vernichten. Angesichts der Sensibilität von Gesundheitsdaten als einer besonderen Kategorie personenbezogener Daten (vgl. Art. 9 der Europäischen Datenschutz-Grundverordnung – DS-GVO, § 22 des Bundesdatenschutzgesetzes – BDSG) ist bei ihrer Vernichtung auf das Einhalten der rechtlichen Vorgaben besondere Sorgfalt zu verwenden.

Die Pflicht des Verantwortlichen zur und das Recht der betroffenen Person auf Vernichtung folgen aus Art. 17 DS-GVO. Zu beachten sind hier auch die Grundsätze der Datenminimierung und Begrenzung der Speicherdauer (Art. 5 Abs. 1 lit. c und e DS-GVO). Nach diesen Vorschriften müssen Daten, die eine Identifizierung der betroffenen Person ermöglichen, auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein; sie sind grundsätzlich nur so lange zu speichern, wie es für Zwecke, für die sie verarbeitet werden, erforderlich ist. Weitere datenschutzrechtliche Regelungen enthalten das BDSG und die Landesdatenschutzgesetze (in Sachsen-Anhalt das Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA) und ggf. bereichsspezifische Regelungen, z. B. in den Landeskrankenhausgesetzen. Zu beachten sind neben den Vorgaben des allgemeinen Datenschutzrechtes zudem weitere gesetzliche und standesrechtliche Bestimmungen, z. B. im Bürgerlichen Gesetzbuch (BGB) zu Haftungsfragen oder in den Berufsordnungen der jeweils zuständigen Kammern zur Schweige- und Dokumentationspflicht. Das Patienten-geheimnis ist durch § 203 des Strafgesetzbuches (StGB) zudem strafrechtlich geschützt.

Solange die Daten einer gesetzlichen, satzungsgemäßen oder vertraglichen Aufbewahrungspflicht unterliegen (Näheres dazu im Folgenden), dürfen sie allerdings (noch) nicht gelöscht werden. Sie können zudem gemäß Art. 9 Abs. 2 lit. f DS-GVO weiterhin aufbewahrt werden, solange der/die Verantwortliche sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen weiterhin benötigt. In diesen und den weiteren in Art. 17 Abs. 3 DS-GVO geregelten Ausnahmefällen dürfen die

Daten dann aber nur noch zur Erfüllung dieser eingeschränkten Zwecke verarbeitet werden. In den Fällen des Art. 18 DS-GVO kann die betroffene Person ihrerseits die Einschränkung der Datenverarbeitung verlangen. In diesem Fall dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur noch mit Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Zur Umsetzung dieser eingeschränkten Verarbeitung sollten die Unterlagen gesondert aufbewahrt, zumindest aber besonders gekennzeichnet werden.

Weitere Ausnahmeregelungen gelten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit und für im öffentlichen Interesse liegende wissenschaftliche Forschungszwecke gemäß Art. 89 DS-GVO (Art. 5 Abs. 1 lit. e, Art. 17 Abs. 3 lit. c und d DS-GVO). Die längere Speicherung für diese Zwecke erfordert ebenfalls die Prüfung, ob und wie lange die Daten hierfür noch erforderlich sind. Die weitere Speicherung für Forschungszwecke nach Art. 89 DS-GVO steht zudem ausdrücklich unter dem Vorbehalt, dass geeignete technische und organisatorische Maßnahmen ergriffen werden. Diese Maßnahmen sollen insbesondere den Grundsatz der Datenminimierung gewährleisten, z. B. durch Pseudonymisierung.

Im Folgenden finden Ärztinnen, Ärzte und andere medizinische Einrichtungen Anregungen und Vorschläge, die ihnen bei einer ordnungsgemäßen Datenvernichtung helfen.

### Was ist zu vernichten?

Der Pflicht zur Vernichtung unterliegen alle Daten, die sich auf eine identifizierbare Person beziehen (vgl. zur Definition der personenbezogenen Daten Art. 4 Nr. 1 DS-GVO). Dazu gehören Unterlagen der Anamnese, Diagnose und Therapie. Einen besonderen Schutz bei der Vernichtung genießen damit nicht etwa nur Karteikarten bzw. Behandlungsakten, Untersuchungsberichte oder Aufnahmen aus bildgebenden Verfahren (z. B. Röntgen-

bilder). Auch bei Telefonnotizen, Terminkalendern, Listen, Briefumschlägen mit Adressangaben, Telefaxen und Fehldrucken oder Fehlkopien ist zu prüfen, ob sie einen Bezug zu Patientinnen oder Patienten aufweisen und daher anstelle einer Entsorgung im Altpapier eine sofortige gesicherte Vernichtung im Reißwolf notwendig ist.

Zunehmend liegen in medizinischen Einrichtungen neben oder anstelle von Unterlagen in Papierform personenbezogene Daten auch in elektronisch gespeicherter Form vor, die zu gegebener Zeit vernichtet werden müssen. Beispiele für Datenträger sind Festplatten (auch mobile), CDs, DVDs und USB-Sticks. Auch Daten aus Programmen (z. B. E-Mailprogrammen) sind zu löschen.

Als weitere Datenträger fallen in Arztpraxen, Krankenhäusern und vor allem in medizinischen Laboren Gewebe- und Blutproben an. Bei den Proben selbst handelt es sich zwar nicht um personenbezogene Daten. Sobald aber eine Kennzeichnung erfolgt ist, aus der genetische oder sonstige medizinische individualisierbare Erkenntnisse - also personenbezogene Daten - abgeleitet werden können, sind auch sie datenschutzkonform zu vernichten.

#### Wann ist zu vernichten?

Der Zeitpunkt der Vernichtung hängt von der Art des personenbezogenen Datums ab. Art. 17 Abs. 1 lit. a und d DS-GVO regeln, dass personenbezogene Daten zu löschen sind, wenn ihre Verarbeitung – also auch die (weitere) Speicherung – unrechtmäßig ist oder wenn die Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind, d. h. sobald ihre Kenntnis für die Aufgabenerfüllung der Arztpraxis bzw. medizinischen Einrichtung nicht mehr erforderlich ist. Die Speicherdauer hat sich also grundsätzlich danach zu richten, wie lange die Daten für Behandlungszwecke bzw. zur Vertragserfüllung benötigt werden.

Eine über die Dauer der Behandlung hinausgehende Aufbewahrung wird erforderlich, wenn sie spezialgesetzlich angeordnet ist. Den allgemeinen Datenschutzgesetzen vorrangig gelten zahlreiche besondere Aufbewahrungspflichten, die stets einzuhalten sind. Beispielsweise gilt zivilrechtlich (§ 630f Abs. 3 BGB) und standesrechtlich (nach den Berufsordnungen für die in Deutschland tätigen Ärztinnen und Ärzte) einheitlich eine zehnjährige Dokumentationspflicht für die ärztlichen Aufzeichnungen, beginnend mit dem Abschluss der Behandlung. Für sogar 30 Jahre aufzubewahren sind nach § 85 des Strahlenschutzgesetzes Aufzeichnungen über die Behandlung mit ionisierender Strahlung oder radioaktiven Stoffen sowie Röntgenbilder, digitale Bilddaten und sonstige Untersuchungsdaten. Für Apotheken finden sich zahlreiche Detailregelungen in der Verordnung über den

Betrieb von Apotheken (Apothekenbetriebsordnung). Besondere Vorgaben enthält auch das Betäubungsmittelrecht. Dies sind nur einige von vielen Beispielen für Spezialregelungen. Die jeweils zuständigen Kammern oder (Berufs-) Vereinigungen bieten häufig Aufstellungen über die im Einzelnen geltenden Aufbewahrungsfristen an<sup>1</sup>.

Allgemeine handels- und steuerrechtliche Aufbewahrungspflichten sind zusätzlich zu beachten. So sind nach § 257 des Handelsgesetzbuches sowie § 147 der Abgabenordnung Buchungsbelege für die Dauer von 10 Jahren, Handels- und Geschäftsbriefe sowie sonstige für die Besteuerung relevante Unterlagen für 6 Jahre aufzubewahren. Dies schließt in diesen Unterlagen befindliche personenbezogene Daten ein.

Über diese Fristen hinaus ist eine Speicherung personenbezogener Gesundheitsdaten regelmäßig unzulässig. Anderes kann dann gelten, wenn die weitere Speicherung zur Verteidigung von Rechtsansprüchen erforderlich ist. Dies kann z. B. der Fall sein, wenn die Gefahr der Geltendmachung von Schadensersatzansprüchen besteht. Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, verjähren in 30 Jahren von dem den Schaden auslösenden Ereignis an, ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis (§ 199 Abs. 2 BGB). Ob es aber wegen der theoretischen Möglichkeit, nach bis zu 30 Jahren noch in Anspruch genommen zu werden, auch datenschutzrechtlich erforderlich ist, ärztliche Dokumentationen entgegen dem Löschungsgebot von Art. 17 DS-GVO länger für eventuelle Haftungsverfahren aufzubewahren, ist im Einzelfall zu prüfen. Voraussetzung für eine entsprechend längere Aufbewahrung ist, dass nachweislich konkrete Anhaltspunkte dafür bestehen, dass mit der Geltendmachung zivilrechtlicher Ansprüche noch zu rechnen ist. Eine rein theoretische Möglichkeit einer Geltendmachung vermag die Erforderlichkeit und damit Zulässigkeit weiterer Speicherung nicht zu begründen. Ansprüche werden in der Regel deutlich vor Ablauf der Verjährungsfrist geltend gemacht. Zudem muss den jeweiligen Daten eine Beweisfunktion zukommen. Das ist regelmäßig nur bei den dokumentationspflichtigen Anamnese-, Diagnose- und Therapiedaten der Fall, kaum jedoch bei sonstigen Aufzeichnungen. Sind die Unterlagen datenschutzgerecht vernichtet, darf der medizinischen Einrichtung daraus kein Nachteil entstehen<sup>2</sup>. Eine Notwendigkeit zur Beweissicherung fehlt des Weiteren, wenn die betroffene Person vorher die Datenvernichtung selbst verlangt hat. Sich in einem solchen Fall in einem Prozess auf eine Beweispflicht der medizinischen Einrichtung zu berufen, wäre treuwidrig und daher unzulässig.

Zusammenfassend ist beim Zeitpunkt der Vernichtung zu unterscheiden:

- Grundsätzlich gilt das Lösungsgebot des Art. 17 DS-GVO, sobald die Daten nicht mehr benötigt werden. Dann hat eine Aufbewahrung längstens für die Dauer der Behandlung zu erfolgen.
- Spezialgesetzliche Aufbewahrungs- und Dokumentationspflichten (z. B. standes-, steuer- oder handelsrechtliche) sind einzuhalten, z. B. die Zehn-Jahres-Frist nach § 10 Abs. 3 der Berufsordnung der Ärztekammer Sachsen-Anhalt.
- Ist nach Ende dieser Aufbewahrungsfristen ausnahmsweise ein Haftungsprozess konkret zu erwarten, ist eine Aufbewahrungsfrist von bis zu 30 Jahren möglich.

Bei verlängerten Aufbewahrungsfristen ist zu beachten, dass die Daten in der Verarbeitung einzuschränken sind, wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nach Abschluss der Behandlung nicht mehr erforderlich ist (siehe Ausführungen in den Vorbemerkungen).

Die Lösfristen sollten idealerweise automatisiert in der Anwendung überwacht werden oder zumindest prozessual geregelt sein, z. B. durch interne Anweisung, dass zu festgelegten Stichtagen regelmäßig manuell zu löschen ist. Von besonderer Bedeutung ist dabei die Kennzeichnung der Daten mit dem Zeitpunkt, zu dem die Fristen beginnen bzw. enden.

#### Wie ist zu vernichten?

Für die Vernichtung von Daten der Patientinnen und Patienten – also allen Datenträgern in Papierform, aber auch in magnetischer Form (Festplatten, Magnetbänder) oder in optischer Form (insbesondere CDs, DVDs) – wurden in DIN 66399 (Büro- und Datentechnik – Vernichten von Datenträgern) in Abhängigkeit von Schutzbedarf und Schutzklasse des Vernichtungsgutes verschiedene Sicherheitsstufen festgelegt. Die Sicherheitsstufen bestimmen je nach Sensibilität des zu vernichtenden Materials bzw. Schutzklasse unterschiedliche Grenzwerte für Zustand, Form und Größe der nach der Vernichtung verbleibenden Materialteilchen. Die Einteilung nach DIN 66399 erfolgt in drei Schutzklassen: 1 (normaler Schutzbedarf), 2 (hoher Schutzbedarf) und 3 (sehr hoher Schutzbedarf). Informationsträger mit besonders sensiblen personenbezogenen Daten, wozu auch medizinische Daten zählen, werden in Schutzklasse 2 oder 3 einzugruppiert sein. Deshalb sollte eine Vernichtung solcher Datenträger mindestens nach Sicherheitsstufe 4 sichergestellt sein, nach der die Reproduktion der Daten nur unter außergewöhnlich hohem Aufwand (Personen, Hilfsmit-

tel, Zeit) möglich wäre. Aus Sicht des Datenschutzes wünschenswert wäre eine Vernichtung nach der Sicherheitsstufe 5. In dieser Sicherheitsstufe wäre die Reproduktion der Daten nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen sowie forensischer Methoden möglich.

Bereits vor der eigentlichen Vernichtung ist darauf zu achten, dass die zu vernichtenden Unterlagen bzw. Datenträger nicht ungesichert lagern, sondern vor dem Zugriff Unberechtigter geschützt sind. Anstatt diese Medien etwa in einem allgemein zugänglichen Ablagefach zu sammeln, sollte ein verschlossener Raum oder ein verschlossenes Behältnis gewählt werden. Eine geeignete Maßnahme, um (vor allem mobile) elektronische Datenträger gegen den Zugriff Unbefugter zu schützen, ist die Verschlüsselung<sup>3</sup>.

Ein Arzt, eine Ärztin oder andere Verantwortliche müssen die Datenträger nicht selbst vernichten. Sie können diese Arbeiten auch Beschäftigten übertragen oder Unternehmen beauftragen, die sich auf die Vernichtung von Datenträgern spezialisiert haben. Vernichtet die medizinische Einrichtung selbst, müssen bei der Wahl der entsprechenden Geräte zur Datenträgervernichtung die Anforderungen der DIN 66399-2 (Büro- und Datentechnik – Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern) berücksichtigt werden. Das so vernichtete Material kann der normalen Abfallentsorgung zugeführt werden.

Entscheidet sich die medizinische Einrichtung für eine Vernichtung durch ein externes Unternehmen, bedarf es datenschutzrechtlich eines Auftragsverarbeitungsvertrages nach Art. 28 Abs. 3 DS-GVO<sup>4</sup>. Es muss vertraglich abgesichert sein, dass die Vernichtung durch das Unternehmen den geschilderten Anforderungen der DIN 66399 entspricht. Zudem muss unter Berücksichtigung des strafrechtlich geschützten Patientengeheimnisses sichergestellt sein, dass keine unbefugte Offenbarung im Sinne des § 203 StGB an die Beschäftigten des Entsorgungsunternehmens erfolgt. Nach Einführung des § 203 Abs. 3 Satz 2 und Abs. 4 StGB ist dies über vertragliche Absicherungen möglich. Es ist dafür Sorge zu tragen, dass die so genannten „mitwirkenden Personen“ bei dem Entsorgungsunternehmen zur Geheimhaltung verpflichtet wurden (vgl. § 203 Abs. 4 StGB). Gleichwohl dürfen den mitwirkenden Personen nur die Daten offenbart werden, die für deren Tätigkeit erforderlich sind. Wenn Daten lediglich vernichtet werden sollen, müssen sie jedoch den mitwirkenden Personen in der Regel nicht bekannt sein. Daher empfiehlt sich die Übergabe des Vernichtungsgutes an das Entsorgungsunternehmen in verschlossenen Behältnissen, die ohne weitere Möglichkeit zur Kenntnisnahme der Daten der Patientinnen und Patienten unmit-

telbar der Vernichtung zugeführt werden. Elektronische Datenträger sollten idealerweise vor der Übergabe an das Entsorgungsunternehmen physisch zerstört werden.

Elektronische Datenträger können nach der Datenlöschung unter Umständen auch in der eigenen Einrichtung weiterverwendet werden. Um die zuvor darauf gespeicherten Daten als gelöscht ansehen zu können, reicht bei verschlüsselten Datenträgern allein das Löschen des zugehörigen Schlüssels nicht aus, vor allem wegen möglicher technischer Fehler beim Löschen und dem zu erwartenden technischen Fortschritt beim Entschlüsseln. Bei Festplatten und USB-Sticks ist daher stets ein vollständiges Überschreiben der Datenträger notwendig; einmaliges Überschreiben reicht. Unter Windows wird dazu z. B. das „cipher“-Werkzeug angeboten. Dabei kann es passieren, dass einzelne Datenblöcke als fehlerhaft markiert und dem Zugriff des Betriebssystems entzogen werden. Solche Blöcke sind ab diesem Zeitpunkt nicht mehr beschreibbar, oft aber noch forensisch auslesbar. Einige Datenträger enthalten unter Umständen versteckte Bereiche, die noch Daten enthalten können. Einer Weiternutzung in der gleichen Einrichtung steht dies in der Regel nicht entgegen. Eine Weitergabe von Festplatten oder USB-Sticks an externe Dritte zur Weiternutzung darf aus diesen Gründen allerdings nicht erfolgen. CDs und DVDs sollten nur einmalig zum Datentransport beschrieben werden<sup>5</sup>.

Möchte ein Verantwortlicher Gesundheitsdaten anonymisiert weiterverwenden, bedarf es auch hierfür einer Rechtsgrundlage, denn auch die Anonymisierung selbst stellt eine Datenverarbeitung dar. Soweit die Anonymisierung eines Datensatzes dadurch erfolgt, dass die identifizierenden Daten gelöscht werden und nur medizinische Restdaten verbleiben, die einer Reidentifizierung nicht zugänglich sind, kann Art. 6 Abs. 1 Satz 1 lit. c DS-GVO i. V. m. der Löschungsverpflichtung des Art. 17 Abs. 1 lit. a DS-GVO einschlägig sein. Dabei kommt der Güte und Gründlichkeit der Anonymisierung eine besondere Bedeutung zu. Denn gemäß Erwägungsgrund 26 zur DS-GVO sind nur diejenigen personenbezogenen Daten nicht weiter von der Anwendung der DS-GVO betroffen,

die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Ob es sich wirklich um anonymisierte Daten handelt, hängt von Art und Umfang der nach dem Anonymisierungsvorgang verbleibenden Daten ab. Häufig vermuten Verantwortliche, dass die Daten bereits beim Entfernen von Namen und Identifikationsnummern aus einem Datensatz anonym seien. Untersuchungen haben allerdings gezeigt, dass vermeintlich anonymisierte Daten häufig allein anhand scheinbar unspezifischer Merkmale (z. B. Postleitzahl, Geburtsdatum und Geschlecht), ggf. in Kombination mit weiteren öffentlich zugänglichen Informationen, wieder Personen eindeutig zugeordnet werden können.

Unabhängig davon, wie die Löschung personenbezogener Daten technisch und organisatorisch umgesetzt wird, sollte jeder Prozess stets nachvollziehbar dokumentiert sein, z. B. durch Löschungs-, Vernichtungs- oder Anonymisierungsprotokolle. Dies ergibt sich aus der Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO.

### Zusammenfassung

Gesundheitsdaten sind datenschutzgerecht vernichtet, wenn

- von der Vernichtung alle Unterlagen mit Bezug auf Daten der Patientinnen und Patienten erfasst sind,
- die Vernichtung zeitnah nach Ablauf der Aufbewahrungsfrist erfolgt sowie
- die datenschutzrechtlichen Sicherheitsanforderungen (insbesondere der DIN 66399) eingehalten werden und bei einer Vernichtung durch beauftragte Dritte die Einhaltung aller Anforderungen vertraglich abgesichert ist.

### Impressum

Herausgeber:  
Der Landesbeauftragte für den  
Datenschutz Sachsen-Anhalt  
Leiterstr. 9, 39104 Magdeburg  
Tel.: (0391) 81803-0  
poststelle@lfd.sachsen-anhalt.de  
<https://datenschutz.sachsen-anhalt.de>  
Stand: Oktober 2020



<sup>1</sup> Informationen für Ärzte in Sachsen-Anhalt sind z. B. abrufbar unter [https://www.kvsa.de/fileadmin/user\\_upload/PDF/Aufbewahrung\\_KVSA.pdf](https://www.kvsa.de/fileadmin/user_upload/PDF/Aufbewahrung_KVSA.pdf) und für Apotheker in Sachsen-Anhalt unter <https://www.ak-sa.de/service/materialien-und-vorlagen/dokument.html?idfile=5039ad63-d7f7-b43b-e1ff-5a4f51738e03>.

<sup>2</sup> Vgl. für die Arzthaftung die Urteile des Oberlandesgerichts Hamm vom 29. Januar 2003, Az. 3 U 91/02, und des Oberlandesgerichts Karlsruhe vom 11. Februar 2004, Az. 7 U 174/02; vgl. weiter ausführlich im XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt, Nr. 10.1.9, abrufbar unter <https://lsaur.de/LfDTBXI>.

<sup>3</sup> Ein Informationsblatt zum Thema „Wie schützt man Datenträger gemäß Datenschutz-Grundverordnung?“ ist abrufbar unter <https://lsaur.de/Datentraegerschutz>.

<sup>4</sup> Eine Formulierungshilfe ist abrufbar unter <https://lsaur.de/AVVGesDatVern>

<sup>5</sup> Aktuelle technische Empfehlungen gibt das BSI unter: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html).