

Robert Kazemi

Daten- und Akten-vernichtung in Krankenhäusern und Arztpraxen

Regeln im Umgang mit Alt-Daten und -Akten



Diese eBroschüre wird unterstützt von:

HSM® **IDEAL**



Deutscher
Ärzte-Verlag

R. Kazemi

Daten- und Akten-vernichtung in Krankenhäusern und Arztpraxen

Regeln im Umgang mit Alt-Daten und -Akten

Von

Dr. Robert Kazemi, Rechtsanwalt, Bonn

Dr. Robert Kazemi, Rechtsanwalt in Bonn, arbeitet seit Jahren auf dem Gebiet des Datenschutzrechts und ist Autor zahlreicher Fachpublikationen, unter anderem des beim Deutschen Anwaltverlag erschienenen Werkes „Datenschutz in der anwaltlichen Beratung“. Er veröffentlicht regelmäßig zu Fragen des Kunden- und Gesundheitsdatenschutzes und ist zudem beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch).

Als ständiger Autor in den gängigen Fachzeitschriften auf dem Gebiet des Medizinrechts (u. a. die MedR und die GesR) beschäftigt sich Herr Dr. Kazemi wissenschaftlich seit vielen Jahren mit Rechtsfragen des Gesundheits- und Medizinrechts. Im Mittelpunkt seiner Arbeit stehen vor allem standes-, berufs- und zulassungsrechtliche Probleme. Die Publikationstätigkeit richtet sich dabei nicht nur an die im Bereich des Medizinrechts tätigen Kollegen, sondern auch an Sie als Leistungserbringer im Gesundheitswesen. Die langjährige wissenschaftliche Auseinandersetzung mit den zahlreichen Problemen auf dem Gebiet des Medizinrechts bietet die Grundlage für eine umfassende Beratung im Gesundheitswesen. Im Rahmen der täglichen Arbeit steht die strategische und konzeptionelle Beratung von Leistungserbringern häufig im Vordergrund. Gemeinsam mit den Mandanten entwickelt Herr Dr. Kazemi zielorientierte Strategien und unterstützt Sie juristisch bei der Verwirklichung Ihrer unternehmerischen Ziele im laufenden Praxis- und Krankenhausbetrieb.

Haftungsausschluss

Die in der eBroschüre enthaltenen Informationen wurden sorgfältig recherchiert und geprüft. Für die Richtigkeit der Angaben sowie die Befolgung von Ratschlägen und Empfehlungen kann der Verlag dennoch keine Haftung übernehmen.

Sonderausgabe für Deutscher Ärzte-Verlag GmbH, Köln 2016, www.aerzteverlag.de
mit freundlicher Genehmigung

Copyright 2016 by Freie Fachinformationen Markus Weins GmbH, Köln

Satz: Helmut Rohde, Euskirchen

Titelabbildung: © M. Schuppich / fotolia.com

Alle Rechte vorbehalten. Abdruck, Nachdruck, Datentechnische Vervielfältigung und Wiedergabe (auch auszugsweise) oder Veränderung über den vertragsgemäßen Gebrauch hinaus bedürfen der schriftlichen Zustimmung des Verlages.

Deutscher Ärzte-Verlag Köln

Inhaltsverzeichnis

1	Geschredderte Patientenakten als Wurfmaterial im Karneval . . .	4
2	Schweigepflicht und Patientengeheimnis ernst nehmen – bei Verstößen droht Freiheitsstrafe bis zu einem Jahr oder Geldstrafe	4
3	Aktenvernichtung ist Datenverarbeitung	5
4	Auswahl der mit der Aktenvernichtung beauftragten Personen	6
5	Einsichtnahmen bei der Datenträger- und Aktenvernichtung weitgehend verhindern	8
6	Welche Sicherheitsstandards sind einzuhalten?	9
7	Regeln zur Datenträger- und Aktenvernichtung	10



Wir schenken Ihnen Zeit. Machen Sie damit, was Sie möchten.

HSM SECURIO AF: Sicher und zeitsparend Akten vernichten – mit automatischem Papiereinzug!

www.hsm.eu

QR Code zum Produktvideo



HSM GmbH + Co. KG · 88699 Frickingen / Germany
Gratis Hotline 00800 44 77 77 66 · info@hsm.eu



HSM®

Great Products, Great People.

1 Geschredderte Patientenakten als Wurfmaterial im Karneval

Die „fünfte Jahreszeit“, nicht nur für den Rheinländer oft ein fester Termin im Kalender, ist gerade erst zu Ende gegangen. Insbesondere in der Hochsaison zwischen Weiberfastnacht und Aschermittwoch wird viel gefeiert und werden nicht nur in Sachen der Trinkfestigkeit und des „guten Geschmacks“, sondern auch in Sachen des Datenschutzrechts gelegentlich Grenzen überschritten. Was die Trinkfestigkeit oder andere moralische Aspekte angeht, mögen Sünden zusammen mit dem „Nubbel“ und dem „Hoppeditz“ einfach verbrannt und hinter sich gelassen werden können; Rechtsverstöße hingegen lassen sich so kaum beseitigen, denn auch in der „nährischen Zeit“ gelten die Gesetze fort. Dies wird wohl nun auch einem MVZ-Betreiber im Wartburgkreis gewahr werden, dessen Mitarbeiter es mit der Feierlust wohl etwas übertrieben haben: Wie u. a. die [BILD-Zeitung](#) und der [MDR](#) berichten sind in der Karnevalszeit Patientenakten geschreddert und das Substrat hieraus als Wurfmaterial genutzt worden. Anders als es die Überschrift „DATEN-SKANDAL! Patientenakten als Faschings-Konfetti“ vermuten lässt, war hier dummerweise wohl

kein Aktenvernichter der Sicherheitsstufen P-4 oder P-5, sondern eher die Haushaltsvariante im Einsatz, die die Patientenakten in feine, aber mit hinreichender Geduld auch wieder zusammensetzbare Streifen geschnitten hatte, sodass Namen, Patientennummern und z. T. sogar Diagnosen weiterhin lesbar gewesen sind. Auch Teile von Röntgenbildern, Dienst- und Einsatzplänen sollen gefunden worden sein. Nun ermittelt Thüringens Landesdatenschutzbeauftragter, vielleicht auch bald die Staatsanwaltschaft. In der Presse heißt es hierzu, man gehe davon aus, dass „[Gedankenlosigkeit im Spiel gewesen sei, aber keine Absicht](#)“. Zum Glück, möchte man auf den ersten Blick meinen, muss dann jedoch schnell zugestehen, dass es dort wo es um das Patientengeheimnis, Gesundheits- und Mitarbeiterdaten, das BDSG spricht allgemeiner von besonderen Arten personenbezogener Daten, geht, auch Gedankenlosigkeit nicht entschuldbar ist. Grund genug, die rechtlichen Rahmenbedingungen der Daten- und Aktenvernichtung in der Arztpraxis und im Krankenhaus zu beleuchten und die notwendige Sensibilität für diesen Themenkomplex zu schärfen.

2 Schweigepflicht und Patientengeheimnis ernst nehmen – bei Verstößen droht Freiheitsstrafe bis zu einem Jahr oder Geldstrafe

Hierbei geht es zunächst darum, sich nochmals die Grundlagen der ärztlichen Schweigepflicht und des Patientengeheimnisses zu vergegenwärtigen. Die ärztliche Schweigepflicht ist wesentliches Merkmal der besonderen Vertrauensbeziehung zwischen Arzt und Patient und damit eine der tragenden Säulen des Arzt-Patienten-Verhältnisses.

Neben seiner besonderen Erwähnung in den Berufsordnungen (vgl. § 7 MBO ZÄ, § 9 MBO Ä), sind die ärztliche Schweigepflicht (§ 203 StGB) und korrespondierend hierzu auch das ärztliche Schweigerecht (§ 53 StPO) auch in den Strafgesetzen berücksichtigt worden. Nach § 203 Abs. 1 Nr. 1 StGB handeln Ärzte, Zahnärzte, Tierärzte,

Apotheker oder Angehörige eines anderen Heilberufs strafbar, wenn sie unbefugt ein fremdes Geheimnis, das ihnen im Rahmen ihrer Berufsausübung anvertraut oder sonst bekannt geworden ist, Dritten gegenüber offenbaren. Die ärztliche Schweigepflicht (§ 203 StGB) gilt dabei grundsätzlich gegenüber jedermann. Sie erstreckt sich dabei nicht nur auf die erhobenen medizinischen Befunde, die Diagnose und die Therapie; vielmehr unterliegt bereits der Umstand, dass ein Behandlungsverhältnis besteht, der Schweigepflicht. Dies hat beispielsweise zur Folge, dass der Arzt oder das Krankenhaus auch Liquidationen mit entsprechender Diagnose nur an den Patienten selbst verschicken darf. Auch bei einem mitversicherten Familienangehörigen ist die Post an den behandelten, nicht an den Hauptversicherten zu richten. Daher kommt auch eine Mithaftung des Ehegatten für Honorarforderungen grundsätzlich nur bei unaufschiebbaren und sachlich gebotenen medizinischen Leistungen und nur dann in Betracht, wenn die Einkommens- und Vermögensverhältnisse des anderen Ehegatten eine Kostentragung von vornherein ausgeschlossen erscheinen lassen. Nach allgemeiner Meinung gilt die Schweigepflicht des Arztes auch in Bezug auf Minderjährige, solange und soweit diese über die notwendige Einsichtsfähigkeit verfügen, was nach allgemeiner Meinung bei

Kindern- und Jugendlichen über 14 Jahren regelmäßig der Fall sein soll. Kurz gesagt: Die ärztliche Schweigepflicht ist extensiv anzuwenden. **Dem Arzt, dem Krankenhaus oder dem ärztlichen Hilfspersonal, das unbefugt, d.h. ohne Einwilligung des Patienten, Behandlungsdaten offenbart, drohen Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.**

Als besonders sensitive Daten unterliegen Gesundheitsdaten auch datenschutzrechtlich einer besonderen Handhabung (§ 3 Abs. 9 BDSG). Der Europäische Gerichtshof hat den Begriff der Gesundheit extensiv dahin ausgelegt, dass dieser alle Informationen erfasse, welche die Gesundheit – körperlich wie auch psychisch – betreffen. Diese Daten unterliegen einer „besonderen Geheimhaltung“, die der Übermittlung an Dritte grundsätzlich entgegensteht. Nur dort, wo ein Bezug zur sozialen Umwelt besteht, soll das Interesse an einer Geheimhaltung sensibler Daten durch andere Interessen überwogen werden können, weswegen notwendige Einschränkungen der Nutzung zu akzeptieren sind, soweit der Verwendungszweck dies rechtfertigt. Gleichwohl dürfen auch besondere Arten personenbezogener Daten nur dann erhoben, verarbeitet und genutzt werden, soweit das Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG).

3 Aktenvernichtung ist Datenverarbeitung

Nachdem unter Datenverarbeitung jeder Prozess, bei dem Daten mit oder ohne technische Hilfsmittel erfasst (erhoben), gespeichert, verändert, übermittelt, gesperrt oder gelöscht werden, zu verstehen ist, handelt es sich auch bei der Aktenvernichtung um einen datenschutzrechtlich relevanten Vorgang. Nicht nur mit Blick auf die besonde-

ren Bestimmungen des Datenschutzrechts, sondern auch mit Blick auf die Reichweite der skizzierten ärztlichen Schweigepflicht ist daher genau darauf zu achten, dass im Rahmen der Datenträger- und Aktenvernichtung keine Gesundheitsdaten an unbefugte Dritte offenbart werden.

4 Auswahl der mit der Aktenvernichtung beauftragten Personen

Eine Offenbarung in diesem Sinne liegt vor, sobald einem Dritten ein Wissen vermittelt wird, das diesem noch verborgen ist oder von dem er jedenfalls noch keine sichere Kenntnis hat. Da der Arzt und das Krankenhaus jedoch grundsätzlich nicht allein und ohne entsprechende Unterstützung von Mitarbeitern tätig werden können, liegt ein strafbares Offenbaren nur dann vor, wenn das Geheimnis aus der Sphäre des Geheimnisträgers hinausgelangt. Der Straftatbestand wird daher dann nicht verwirklicht, wenn das Geheimnis lediglich im Kreis der zum Wissen Berufenen mitgeteilt wird. Ein strafrechtlich relevantes „Offenbaren“ scheidet deswegen nach ganz herrschender Meinung gegenüber Hilfskräften (berufsmäßig tätige Gehilfen) des schweigepflichtigen Arztes aus. Die angestellte Arzthelferin oder der angestellte Krankenpfleger darf daher nicht nur über den Umstand des Bestehens eines Behandlungsverhältnisses, sondern auch über den Inhalt desselben grundsätzlich ohne Einwilligung des betroffenen Patienten informiert werden. § 203 Abs. 3 S 1 StGB bezieht diese dauerhaft in die Praxis- bzw. Krankenhausorganisation eingegliederten ärztlichen Hilfspersonen folgerichtig in die ärztliche Schweigepflicht mit ein; auch die an die ärztlichen Gehilfen mitgeteilten Informationen (Geheimnisse) unterliegen einem entsprechenden Aussage- oder Zeugnisverweigerungsrecht (§ 53a StPO).

Fraglich ist jedoch, wer unter den Begriff des berufsmäßig tätigen Gehilfen fällt. Unstreitig ist dies nur bei auf Dauer in der Arztpraxis oder dem Krankenhaus fest angestellten Mitarbeitern. Was aber, wenn mit der Aktenvernichtung Dritte beauftragt werden sollen? Diese sind nicht als „Angestellte“ in die Organisation eingebunden und

damit wohl auch nicht als „berufsmäßige Gehilfen“ zu qualifizieren. Ist die Aktenvernichtung damit nur(!) durch Angestellte der Arztpraxis / des Krankenhauses und seine Angestellten möglich und zulässig, ohne sich offenkundig in die Gefahr strafbarer und berufsrechtswidriger Handlungen zu begeben?

Ein erster Blick in die strafrechtliche Literatur lässt hier böses erahnen. So soll nach (noch) herrschender Auffassung im strafrechtlichen Schrifttum eine organisatorische Einbindung des Gehilfen in den Betrieb des Berufsträgers notwendig sein, die sich in einer Weisungsabhängigkeit des Helfers niederschlägt. Auch wenn das Bestehen eines Arbeitsvertrags dabei nicht gefordert wird, soll doch eine (arbeitsrechtlich) faktische, vom Direktionsrecht bestimmte Tätigkeit des Gehilfen zwingend erforderlich sein. Dies umfasst unter anderem das Recht, einseitig insbesondere Inhalt, Ort und Zeit der Arbeitsleitung bestimmen zu können. Dies ist bei externen Dienstleistern eher nicht der Fall, sodass jede Offenbarung von Geheimnissen an diese (ohne Einwilligung des betroffenen Patienten) gleichsam einen strafbaren Verstoß gegen die ärztlichen Geheimhaltungspflichten darstellen würde.

Dass dies nicht richtig sein kann, liegt auf der Hand. Dementsprechend sind in jüngerer Zeit zahlreiche Stimmen gegen das restriktive Verständnis des Gehilfenbegriffs laut geworden. Obgleich auch diese der Beauftragung externer Dienstleister nicht Tür und Tor öffnen wollen, soll der Einsatz externer Dienstleister – das Outsourcing – dennoch straffrei sein, wenn der Arzt eine Steuerungsmacht über den Dienstleister ausüben könne, die ihm die Herrschaft über die dem Dritten zur Verfügung gestellten

Informationen belasse. Ein Blick in die Datenschutzgesetzgebung spricht für ein derartiges Verständnis. Nach § 11 BDSG ist der Datenumgang mit Patientendaten durch externe Dienstleister dann zulässig, wenn das Verhältnis zwischen dem Arzt und dem externen Dienstleister als sog. Auftragsdatenverarbeitung im Sinne von § 11 BDSG ausgestaltet ist. Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten durch eine andere verantwortliche Stelle im Auftrag erhoben, verarbeitet oder genutzt werden (§ 11 BDSG). Die andere Stelle muss dabei den Weisungen des Auftraggebers unterworfen sein und darf keine eigene Entscheidungsbefugnis darüber besitzen, wie sie mit den Daten umgeht (im Gegensatz zur sogenannten Funktionsübertragung). Der Auftragnehmer ist zudem sorgfältig auszuwählen, der Auftrag muss schriftlich erteilt werden und der Auftrag-

geber muss den Auftragnehmer umfassend kontrollieren können und seine Kontrollen schriftlich dokumentieren. Vergibt der Arzt / das Krankenhaus Aufträge an externe Dienstleister ohne eine solche oder im Rahmen einer unzureichenden Auftragsdatenverarbeitungsvereinbarung, stellt dies gleichzeitig eine Ordnungswidrigkeit dar, die mit Ordnungsgeldern in Höhe von bis zu 50.000 € sanktioniert werden kann. Datenschutzrechtlich würde es also genügen, die Tätigkeit externer Dienstleister im Rahmen der Aktenvernichtung als Datenverarbeitung im Auftrag gem. § 11 BDSG auszugestalten.

Dies kann allerdings im Ergebnis auch nicht dazu führen, die Hinzuziehung von (externen) Hilfspersonen unbeschränkt zuzulassen. Vielmehr ist hier in jedem Einzelfall der Gefahr für eine Verletzung des persönlichen Geheimhaltungsinteresses



Sie erheben Lücken schließen.

Auch im Umgang mit äußerst sensiblen Patientendaten ist REISSWOLF als richtungsweisendes Unternehmen für Akten- und Datenträgervernichtung, individuelle Archivleistungen und hochqualitatives Dokumentenmanagement in der Zukunft angekommen. Denn während der gesamten Prozesse ist ein Zugriff auf empfindliche Daten konsequent ausgeschlossen. **Das nennen wir Vorsorge.**



REISSWOLF®
secret. service.

www.reisswolf.de

des Patienten Rechnung zu tragen. Dies erfordert entweder eine konkrete auf den jeweiligen Dienstleister bezogene Einwilligung des betroffenen Patienten oder eine starke Anbindung des externen Dienstleisters an den Geheimnisträger, wodurch sichergestellt wird, dass die Weitergabe an den externen Dienstleister keine Risiken für das Persönlichkeitsrecht des Patienten schafft, die über das mit der Bekanntgabe an den Arzt selbst bereits bestehende Risiko signifikant hinausgehen. In diesem Sinne hat es beispielsweise das Bundesverfassungsgericht im Falle der Einsichtnahme in Patientenakten einer Universitätsklinik durch einen Landesrechnungshof für ausreichend erachtet, dass die Prüfer ihrerseits zur Verschwiegenheit verpflichtet waren. Daraus folgert die Große Strafrechtskommission des Deutschen Richterbundes in einem für das Bundesministerium der Justiz erstatteten Gutachten für das Outsourcing von IT-Dienstleistungen, dass *„eine solche Zusicherung in vertraglicher Hinsicht bei den IT-Firmen als ausreichend angesehen werden müsste.“* (Große Strafrechtskommission des Deutschen Richterbundes, Auslagerung von Dienstleistungen durch Berufsgeheimnisträger und Datenaustausch zwischen Behörden, 2006, 71).

Dies zugrunde gelegt ist es jedenfalls erforderlich, dass der Arzt / das Krankenhaus seine externen Dienstleister in einer Art und Weise in seine Verschwiegenheitsverpflichtung einbindet, die die Wahrung der durch § 203 StGB geschützten Patienteninteressen rechtfertigt. Dies sollte beispielsweise durch eine Verschwiegenheitsverpflichtung geschehen, die auch allen Mitarbeitern des externen Dienstleisters auferlegt wird. Des Weiteren empfiehlt sich die Vereinbarung von Vertragsstrafen für den Fall der Zuwiderhandlung, welche ebenfalls dazu geeignet sind, solche im Vorfeld auszuschließen bzw. die Gefahr solcher Zuwiderhandlungen im Vorfeld erheblich zu minimieren. Auch wenn weder die Rechtsprechung noch der Gesetzgeber sich bislang dazu geäußert haben, ob eine solche Vorgehensweise tatsächlich zu einem objektiven Strafbarkeitsausschluss zugunsten des betroffenen Arztes führt, werden derartige Maßnahmen doch sicherlich auf subjektiver Ebene das Strafbarkeitsrisiko erheblich minimieren. Wer hier ohne entsprechende vertragliche Vereinbarungen mit externen Dienstleistern zusammenarbeitet, der könnte schnell Bekanntschaft mit dem Staatsanwalt oder dem Strafrichter machen.

5 Einsichtnahmen bei der Datenträger- und Aktenvernichtung weitgehend verhindern

Um das Risiko weiter zu vermindern und die Zugriffsmöglichkeiten auf Patientendaten durch Dritte so weit wie möglich zu verhindern, sollten Akten und Datenträger zudem niemals „offen“, sondern in verschlossenen Behältnissen übergeben werden, die in der Datenvernichtungsanlage maschinell geöffnet und grundsätzlich ohne menschliche Verarbeitungsvorgänge einer Vernichtung zugeführt werden. Zahlreiche externe An-

bieter von Datenträger- und Aktenvernichtungsdienstleistungen bieten dies an; viele haben die getroffenen Maßnahmen zusätzlich durch unabhängige Stellen auf die Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen überprüfen und von diesen zertifizieren lassen. Hier gilt mehr als sonst, dass hier in keinem Fall allein mit Blick auf Kosten eine Auswahl getroffen werden sollte. Vielmehr sollten bei allzu

günstigen Angeboten eher die Alarmglocken läuten und der Dienstleister vor Beauftragung näher unter die Lupe genommen werden. Das Erfordernis des Unter-die-Lupe-Nehmens gilt jedoch auch dann, wenn ein Anbieter vordergründig seriös erscheint. Auch in diesem Fall tut der Arzt oder das

Krankenhaus gut daran, sich vor Ort von der Vorgehensweise des Dienstleisters zu überzeugen und die Einhaltung der ausgehandelten Sicherheitsstandards bei der Daten- und Aktenträgersvernichtung in regelmäßigen Abständen zu kontrollieren.

6 Welche Sicherheitsstandards sind einzuhalten?

Der eingangs geschilderte „Konfetti-Fall“ macht deutlich, dass „Schreddern“ nicht gleich „Schreddern“ bedeutet. Einfaches, grobes Zerreißen der Akten reicht hier nicht aus. Akten und Datenträger sind vielmehr so zu zerstören, dass ihre Wiederherstellung auch unter größtmöglichen Anstrengungen ausgeschlossen ist. Das BDSG spricht in diesem Sinne vom „Löschen“ und meint damit die endgültige, nicht mehr rückgängig zu machende Vernichtung personenbezogener Daten, die dazu führt, dass die Informationen nicht mehr lesbar gemacht werden können. Wer hier den Stand der Technik beachtet, der orientiert sich jedenfalls an den DIN-Normen EN 15713 und DIN 66399, die Verfahrensregeln zur sicheren Vernichtung von vertraulichen Unterlagen und Datenträgern aufstellen, und greift auf Aktenvernichter der Sicherheitsstufen P-4 oder besser P-5 zurück. Geräte dieser Sicherheitsstufen vernichten die Dokumente so, „*dass eine Rekonstruktion der Information mit hoher Wahrscheinlichkeit ausgeschlossen werden kann*“ (BSI 2013). Erst die so geschredderten Akten oder das, was davon übrig bleibt, kann dann im Papiermüll entsorgt werden. Wer gänzlich auf Nummer sicher gehen will, hat die Möglichkeit, Geräte der Sicherheitsstufe P-7 einzusetzen, die nach getaner Arbeit nur noch Granulat übrig lassen. Dies gilt auch für elektronische Datenträger. Auch diese dürfen nicht einfach auf dem Sperrmüll entsorgt werden, auch das einfache Löschen

des virtuellen Papierkorbs reicht hier nicht aus. Eine sichere Löschung elektronischer Daten ist in diesem Sinne allein durch das mehrfache (mindestens sechsfache) Überschreiben der jeweiligen Festplatte möglich. Sicherer geht zudem, wer den Datenträger nicht nur überschreibt, sondern physisch zerstört, sei es unter Zuhilfenahme eines ordentlichen Hammers oder spezieller Schredder, die von professionellen Aktenvernichtungsdienstleistern vorgehalten werden. In Sachen Patientengeheimnis sollte in diesem Sinne zudem nicht nur an Computer und Medizingeräte, sondern beispielsweise auch an moderne Kopiergeräte mit einer Festplatte gedacht werden, die etwa von der Landesbeauftragten für Datenschutz in Bremen in einer Orientierungshilfe zu Recht als „*angreifbare Datenstation*“ bezeichnet werden. Sie empfiehlt: „*Bei der Entsorgung ausgemusterter Geräte gilt, dass alle Daten, die noch auf dem System verblieben sind beziehungsweise sein könnten, gelöscht werden müssen.*“ Wer solche Geräte gekauft, gemietet oder geleast hat, dem sei das Studium dieser Orientierungshilfe angeraten. Wer hier nicht so weit gehen und seine Alt-Geräte ggf. noch verkaufen oder Dritten zur Verfügung stellen möchte, dem sei dringend das vorherige Studium der Empfehlung des Bundesamts für Sicherheit in der Informationstechnik empfohlen, welche im [Internet](#) abgerufen werden kann.

7 Regeln zur Datenträger- und Aktenvernichtung

Wer die oben beschriebenen Standards beachtet, der stellt sicher, dass die in seinem Betrieb (Krankenhaus oder Arztpraxis) erhobenen Daten auch bei ihrer Vernichtung nicht in die falschen Hände geraten, und vermeidet unliebsame Erwähnungen in der Tagespresse. Da die Narren nicht nur in der Karnevalszeit los sind, sondern „Unachtsamkeit“ stets eine große Gefahr darstellt,

gilt es zudem auch die Mitarbeiterinnen und Mitarbeiter für die Belange des Datenschutzes und der Datensicherheit über regelmäßige Schulungen und Informationen zu sensibilisieren und sensibilisiert zu halten. Die übliche und von Gesetzes wegen geforderte Verpflichtung auf das Datengeheimnis im Arbeitsvertrag (§ 5 BDSG), reicht hierfür sicherlich nicht aus. Im Übrigen gilt:

1. Zur Aktenvernichtung im Krankenhaus und in der Arztpraxis sind Aktenvernichter der Sicherheitsstufe P-4 oder höher zu nutzen.
2. Die Vernichtung digitaler Akten ist durch das einfache Löschen nicht gewährleistet. Auch das einfache Überschreiben der Festplatte reicht nicht. Letztere muss entweder physisch zerstört oder durch eine versierte Drittfirma gelöscht bzw. entsorgt werden. Dies gilt auch für Kopier- und Medizingeräte mit Festplatten und Arbeitsspeicher.
3. Soweit externe Dritte mit der Datenträger- und Aktenvernichtung beauftragt werden, ist sicherzustellen, dass:
 - ▲ eine uneingeschränkte und jederzeitige Dispositionsbefugnis über die die Patienten betreffenden Abläufe gegenüber dem externen Dienstleister („Ob“ und „Wie“) sichergestellt ist;
 - ▲ jeder Arbeitsschritt und jedes Arbeitsergebnis des externen Dienstleisters durch diesen ausreichend dokumentiert und unverzüglich mitgeteilt wird;
 - ▲ Patientendaten auch beim externen Dienstleister durch ausreichende Sicherungsmaßnahmen gegen missbräuchliche Verwendung durch nicht autorisierte Dritte geschützt werden;
 - ▲ die technischen und betrieblichen Abläufe beim Dienstleister so organisiert sind, dass nur streng beschränkte Zugriffsrechte auf die zu vernichtenden Akten gewährt werden;
 - ▲ ausreichende Sicherheitsvorsorge in räumlicher Hinsicht beim externen Dienstleister gewahrt wird;
 - ▲ eine ausreichende Verschwiegenheitsvorsorge durch Schulungen und kontinuierliche Überwachung sowie ausreichende schriftliche Verschwiegenheitserklärungen des externen Dienstleisters gewährleistet werden; und
 - ▲ der externe Dienstleister über eine Auftragsdatenverarbeitungsvereinbarung, die für den Fall des Verstoßes gegen die dort normierten Pflichten erhebliche Vertragsstrafen vorsieht, gebunden ist.

DIN 66399

Die DIN 66399 sorgt für Klarheit beim Datenschutz. Sie stellt genaue Anforderungen an die ordnungsgemäße Datenträgervernichtung, schützt somit wichtige Daten und klärt Ihren konkreten Bedarf. Ihren individuellen Schutzbedarf nach DIN 66399 bestimmen Sie ganz einfach, indem Sie zuerst eine Schutzklasse und dann die für Sie passende Sicherheitsstufe (P: Papier) bestimmen.

Patientendaten sollten mindestens mit Aktenvernichtern der Sicherheitsstufe P-4 vernichtet werden.

Schutzklasse 1 Normaler Schutzbedarf	P-1	Allgemeine Daten	Altes Werbematerial, wie Prospekte & Kataloge. Nicht für personenbezogene Daten geeignet.
	P-2	Interne Daten	Interne Kommunikation, wie Anweisungen, Reiserichtlinien, Formulare. Nicht für personenbezogene Daten geeignet.
Schutzklasse 2 Hoher Schutzbedarf	P-3	Sensible Daten	Angebote, Bestellungen, Auftragsbestätigungen oder Liefer­scheine mit Adressdaten.
	P-4	Besonders sensible Daten	Patientenakten, Röntgenbilder, Arbeitsunterlagen, Kundendaten, Rechnungen.
Schutzklasse 3 Sehr hoher Schutzbedarf	P-5	Geheim zu haltende Daten	Bilanz, Strategiepapiere, Konstruktionsunterlagen, personenbezogene Daten.
	P-6	Geheime Hochsicherheitsdaten	Patente, Forschungs- und Entwicklungsunterlagen, Informationen, die existenziell wichtig sind.
	P-7	Top Secret Hochsicherheitsdaten	Für den militärischen Bereich, Botschaften, Nachrichtendienste.

Die DIN 66399 für Sie auf einem Blick. Mit freundlicher Unterstützung von [IDEAL](#).

ICH SCHÜTZE DATEN!

Die Empfehlung nach **DIN 66399**: Vertrauliche Daten sicher vernichten.

Weil mir nicht nur die Gesundheit meiner Patienten am Herzen liegt, sondern auch deren Intimsphäre.



Datenschutz geht jeden Mediziner an! Der diskrete Umgang mit Patientendaten ist die Verpflichtung einer jeden Arztpraxis. Mit IDEAL sind Sie auf der sicheren Seite: Kompetent in Sachen Datenschutz und absolut zuverlässig in Punkto Qualität und Service.

Erfahren Sie mehr: ideal.de/datenschutz