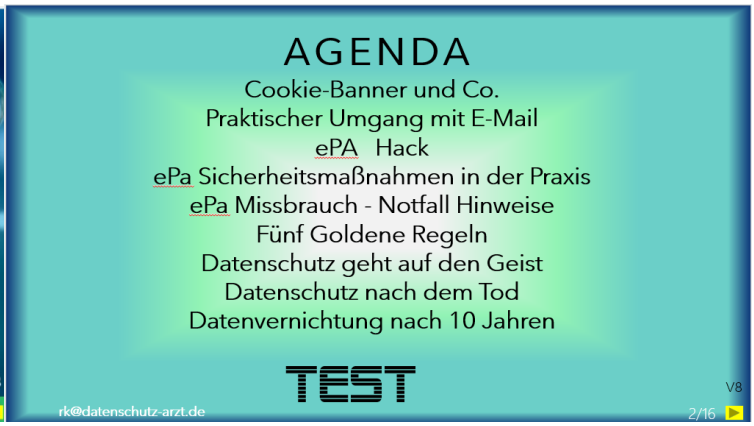
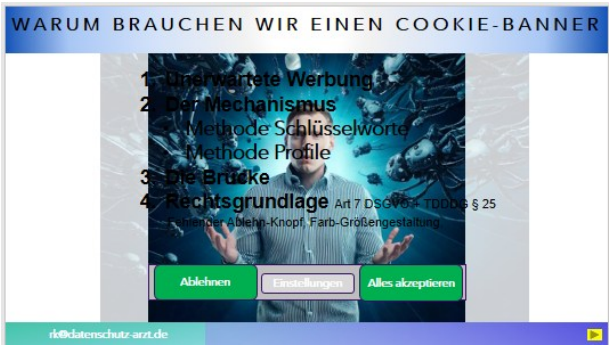




Warum brauchen wir Cookie-Banner und Co.

Cookie-Banner sind die Grundlage für gezielte Werbung.
Das Phänomen: Die unerwartete Werbung

Beispiel:
Ein Nutzer sucht im Internet nach neutralen, alltäglichen oder traditionsbehafteten Begriffen wie "Wienerschnitzel", "Wanderurlaub im Schwarzwald" oder "deutsches Bier".

Ergebnis: Neben den eigentlichen Suchergebnissen erscheint gezielte Werbung z.B. einer bestimmten politischen Partei.

Die erste Reaktion des Nutzers: "Was hat das eine mit dem anderen zu tun? Das muss ein Zufall sein."

Die Realität: Das ist kein Zufall. Es ist das Ergebnis einer ausgeklügelten Strategie der Ziel-Analyse (Targeting).

Der Mechanismus dahinter:

Es gibt zwei Methoden, wie der Werbetreibende (z.B. Partei) den Nutzer erreicht, die oft kombiniert werden:

Methode A: Direkte Schlüsselwort-Analyse (Keyword-Targeting)

Die Partei bucht bei der Werbeplattform (z. B. Google) gezielt Schlüsselworte, die ein bestimmtes Lebensgefühl oder eine Werthaltung transportieren sollen.

Motive: Man will nicht nur politisch Interessierte erreichen, sondern Menschen in ihrem Alltag abholen und eine emotionale Verbindung zu Themen wie "Tradition", "Heimat" oder "Normalität" herstellen. Der Nutzer wird in einem Moment angesprochen, in dem seine "politische Firewall" nicht aktiv ist.

Methode B: Indirektes Profil-Targeting (Hier beginnt der Datenschutz-Aspekt!)

Die Partei schaltet Werbung nicht nur auf Keywords, sondern auf **Nutzerprofile**.
Die Anweisung an die Werbeplattform lautet z. B.: "Zeige meine Werbung an Männer, 40-60 Jahre alt, aus ländlichen Regionen, die sich für traditionelle Rezepte, deutsche Autos und Fußball interessieren."

Die entscheidende Frage ist: Woher kennt die Werbeplattform diese detaillierten Interessen?

Die Brücke: Und hier kommt der Cookie-Banner ins Spiel!

Die Erstellung dieser detaillierten Nutzerprofile ist nur möglich, weil wir im Netz ständig Datenspuren hinterlassen. Die Eintrittskarte dafür ist der Klick auf dem Cookie-Banner „Alles akzeptieren".

Was passiert beim Klick auf "Alles akzeptieren"?

Der Nutzer gibt seine Einwilligung, dass Werbe- und Tracking-Cookies von Drittanbietern (Google, Meta, etc.) auf **seinem Gerät** gespeichert werden dürfen.

Diese Cookies protokollieren nun sein Verhalten: Welche Nachrichtenseiten liest er? Welche Produkte kauft er? Welche Videos schaut er? Welche Rezepte sucht er?
Aus diesen Puzzleteilen entsteht über Wochen und Monate das detaillierte Profil, das für das politische Targeting (Methode B) verwendet wird.

Die Psychologie des Cookie-Banners:

Cookie-Banner sind oft bewusst so gestaltet ("Dark Patterns", Dunkle Muster), dass der Nutzer zur schnellen und umfassenden Zustimmung verleitet wird.
Der **"Alles akzeptieren"-Button** ist groß, farbig und prominent platziert.
Der **"Ablehnen"- oder "Einstellungen"-Button** ist klein, grau, unauffällig oder erfordert mehrere zusätzliche Klicks, was als mühsam empfunden wird.

Fazit:

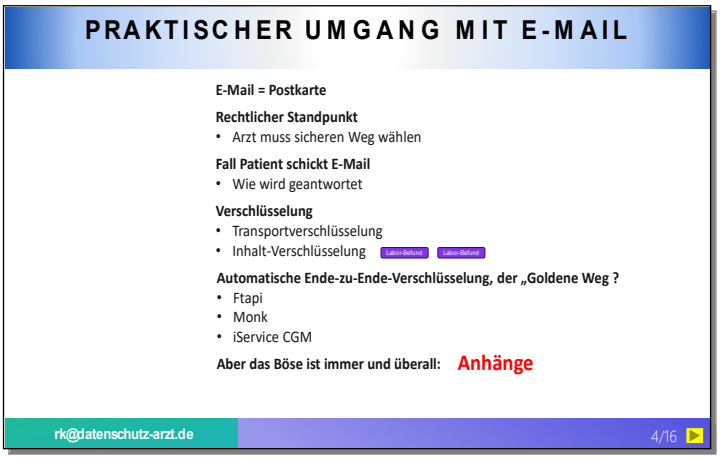
Der Klick auf solch einen "faulen" Cookie-Banner ist nicht harmlos. Er ist der Beginn einer langen Datenverarbeitungskette.
Die "hinterrücks gemachte Besucher-Datenanalyse" ist die Grundlage dafür, dass politische Akteure uns nicht nur mit Sachthemen, sondern gezielt über unsere vermeintlichen Alltagsinteressen und Emotionen ansprechen können.
Das Beispiel "Wienerschnitzel" zeigt perfekt, dass Datenschutz kein abstraktes Thema ist, sondern direkt in die Sphäre der politischen Meinungsbildung hineinreicht.
Eine informierte und freiwillige Einwilligung (wie von der DS-GVO gefordert) ist bei diesen manipulativen Banner-Designs nicht mehr gegeben. Der Nutzer wird über die Tragweite seiner Zustimmung im Unklaren gelassen – genau das ist der "Missbrauch „.

Schutz durch automatisches Löschen von Browser-Daten:

- Diese Einstellung im Browser ist ein sehr wirksamer Basisschutz, der das Erstellen von langfristigen Werbeprofilen über Webseiten hinweg massiv erschwert.
- Die Kette des Cookie-Trackings wird bei jedem Neustart des Browsers unterbrochen, wodurch Sie für Tracker wie ein neuer Nutzer erscheinen.
- Allerdings schützt die Funktion nicht vor Tracking *innerhalb einer einzigen Sitzung* oder vor neueren, Cookie-losen Methoden wie dem Fingerprinting.
- Der erhöhte Datenschutz führt zu einem Komfortverlust, da man sich auf allen Webseiten bei jeder neuen Sitzung erneut anmelden muss.

Rechtlicher Standpunkt:

Solche Cookie-Banner sind ein Datenschutzverstoß. Eine Meldung bei der Aufsichtsbehörde verursacht Bußgeld gegen den Cookie-Banner-Betreiber und zusätzlich die Möglichkeit für den Betroffenen Schadenersatz einzuklagen.



Praktischer Umgang mit E-Mail

E-Mail ist wie eine Postkarte, die von Dritten im Internet leicht gelesen werden kann. Wollen wir das? Wie gehen wir also am einfachsten vor, ohne uns zu verrenken?

Rechtlicher Standpunkt:

Gesundheitsdaten genießen höchste Priorität im Datenschutz. Dies manifestiert sich in Art. 9 DSGVO, der die Verarbeitung von Gesundheitsdaten grundsätzlich verbietet und nur in 10 genau aufgezählten Erlaubnistatbeständen erlaubt.

Grundsätzlich gelten für alle Daten zusätzlich allgemeine Sicherheitsanforderungen:

- Artikel 32, der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

- Artikel 44, bei der Übermittlung an Dritte müssen angemessene Garantien für den Schutz der Daten vorgesehen werden. Dies bedeutet, dass z.B. der Arzt für die Übermittlung der Daten ein sicheres Übermittlungsverfahren verwenden muss.

Unpraktischer aber rechtlich sauberer Ansatz:

Legt ein Patient seine Gesundheitsdaten per E-Mail im Internet offen, so ist dies sein Recht und seine Sache, nicht die des Arztes.

- Antwortet aber ein Arzt darauf, so darf er sich weder auf eine Bewertung der Situation noch auf den Umstand, dass er Arzt ist, einlassen und schon gar nicht die E-Mail-Funktion „Antworten“ seines E-Mail-Programms nutzen, um die Anfrage-E-Mail des Patienten mit seiner Antwort in einen medizinischen Zusammenhang bringen.
- Folge: Verletzung der ärztlichen Schweigepflicht StGB 203, Datenschutzverletzung nach Art. 32 und 44, möglicher Schadensersatzanspruch.

Besser:

- Patient anrufen und Sachverhalt klären, oder
- Antwort mit separater E-Mail, ohne Praxis-Header, ohne Anrede, ohne Vornamen, ohne Gesundheitsdaten.

Beispieltexte

- Aus Datenschutzgründen können wir Ihnen nicht antworten, bitte rufen Sie uns an.
- Bitte kommen Sie persönlich vorbei
- Ihr Terminwunsch ist in Ordnung
- Termin wäre möglich am 01.06.2025 - 16:30, bitte bestätigen Sie, dass es passt.

Verschlüsselung: Transport- vs. Textverschlüsselung

Die **Transportverschlüsselung (TLS)** schützt Ihre Daten auf dem Weg durch das Internet, vergleichbar mit einem Mantel, der ein Lan-Kabel vor äußeren Störungen schützt. Sie sorgt dafür, dass Dritte (z. B. auf dem Weg zwischen Ihrem Computer und dem Server) die E-Mail nicht einfach abfangen und mitlesen können. Dieser Schutz ist wichtig und nach Art. 32 DSGVO gefordert.

Der entscheidende Punkt ist jedoch, dass dieser "Mantelschutz" beim E-Mail-Provider endet. Um die E-Mail korrekt weiterleiten zu können, wird sie dort kurz entschlüsselt, um die Adressdaten auszulesen. Das bedeutet: Der Provider **könnte theoretisch** den Inhalt der E-Mail einsehen. Für sensible Informationen, insbesondere Gesundheitsdaten, ist dies ein unakzeptables Risiko. Datenschützer fordern deshalb, zusätzlich zur Transportverschlüsselung auch eine **Textverschlüsselung (Ende-zu-Ende-Verschlüsselung)**.

Textverschlüsselung: Der Inhalt der E-Mail selbst muss verschlüsselt werden. Die Transportverschlüsselung ist dann nur noch eine sekundäre, aber weiterhin wichtige Schutzebene.

Textverschlüsselung:

Der Inhalt der E-Mail muss also verschlüsselt werden, eine Transportverschlüsselung wäre damit überflüssig bzw. sekundär.

a) US-Ende-zu-Ende-Verschlüsselung.

Die Verschlüsselung muss also, wie bei WhatsApp propagiert, Ende-zu-Ende erfolgen. Die große Frage ist aber: Wer hat den Schlüssel zur Verschlüsselung und könnte die Inhalte deswegen lesen? Das war bei WhatsApp bis 2023 völlig unklar. Erst im April 2023 hat WhatsApp auf Druck der EU-Datenschützer die Funktion „Schlüsseltransparenz“ implementiert, mit der die Verschlüsselung zwischen zwei Kontakten überprüft werden kann. Aktuell tauchen aber hier durch die Nähe und Zugeständnisse des Inhabers Mark Zuckerberg an die aktuelle US-Regierung wieder neue Fragezeichen auf. WhatsApp bleibt dadurch nach wie vor ein Wackelkandidat und ist im Gesundheitswesen nur bedingt möglich.

b) Manuelle Verschlüsselung ist umständlich aber möglich:

Für den Nutzer ist die Handhabung relativ umständlich. Er muss ein Verschlüsselungsprogramm besitzen oder kaufen, seinen Text verschlüsseln und als Anhang versenden und schließlich dem Empfänger den Schlüssel zur Entschlüsselung mitteilen.

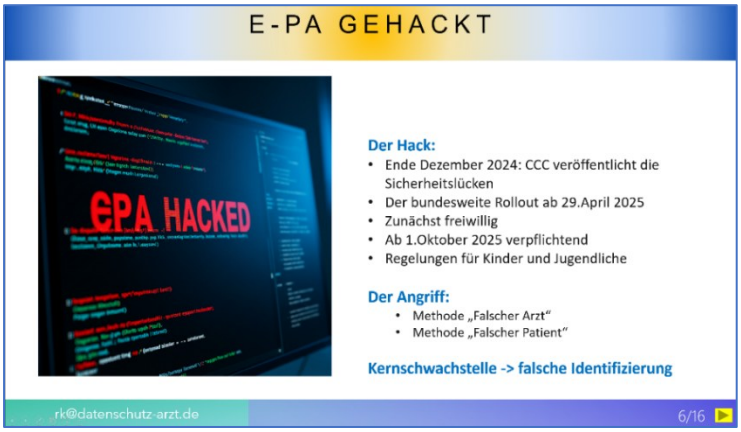
c) Deutsche (EU) Ende-zu-Ende-Verschlüsselung, der „Goldene Weg“?

- **FTapi:** Der Hersteller bietet eine kostenpflichtige Software für den Arzt an. Jedem Patienten, mit dem der Arzt per E-Mail kommunizieren möchte, erhält eine Registrierungs-E-Mail, die beim Patienten einen Zusatz in Microsoft Outlook einmalig installiert. Nun werden alle E-Mails an den Arzt automatisch verschlüsselt. Umgekehrt, wenn der Arzt antwortet, wird die E-Mail beim Patienten automatisch entschlüsselt.
- **Monk:** Eine kostenpflichtige Plattform für Ärzte zum Wissensaustausch zwischen Fachärzten und zur Kommunikation mit dem Patienten. Hier erhält der Patient eine APP, die er ebenfalls installieren muss und die eine Ende-zu-Ende-Verschlüsselung mit der Plattform aufbaut. Hier kann er auf einfache Weise Bilder und Nachrichten ablegen oder, wenn er zuvor per E-Mail benachrichtigt wurde, Informationen in seinem Monk-Postfach abholen. Die Kommunikation läuft also nicht über E-Mail, sonder von der Patienten-App über die Plattform zum Arzt mit einer echten Ende-Zu-Ende-Verschlüsselung. Über E-Mail wird lediglich informiert, „Sie haben eine Nachricht, holen Sie diese mit Ihrer App ab“.
- **Andere**: Manche Hersteller von Praxissoftware, z.B. CGM bieten auf ähnlicher Basis eigene Kommunikationsmodule an, die an deren Software angepasst ist und unter Umständen einen besseren Arbeitsablauf unterstützen. Eine Nachfrage lohnt sich daher.

Aber das Böse ist immer und überall:

Das Sprichwort soll die Menschen ermahnen, vorsichtig zu sein und sich immer bewusst zu sein, was um sie herum passiert. Wir wollen ja nicht nur Worte senden, sondern auch Anlagen mit Bildern und Dateien senden und genau dort steckt das Böse drin, trotz hoher Übertragungssicherheit und Verschlüsselung.
Aus „Sicherheitsgründen“ wird bei den meisten Anbieter daher nur die Übertragung von PDF-Dateien und Bildern erlaubt, denn es ist allgemein bekannt, dass man in Dateien, die mit EXE, DOC, BAT usw. enden, Viren versteckt sein können. Wer aber glaubt, dass in PDF-Dateien oder Bildern(!) keine Viren übertragen werden können, der irrt.
Wichtig: Deshalb sollte bei jedem Dienstleister nachgefragt werden, ob dieser die Kommunikation/Anhänge auf Viren prüft oder einfach nur durchreicht. Lassen Sie sich die Datei-Formate aufzählen, die gescannt werden können. Wenn er auf Viren prüft, fragen Sie auch, ob nach der **„Steganografie-Methode“** analysiert wird. Steganografie ist eine Methode mit der in PDF- Bild-Datei-Formate Schadsoftware versteckt werden kann. Übliche Viren-Scanner spüren diese NICHT auf, sondern dies ist nur mit speziellen Steganografie-Tools möglich.

Ansonsten empfehle ich, die Anhänge über das Virentestportal „Virustotal“ https://www.virustotal.com/ zu testen. Allerdings dort ohne Steganografie-Prüfung.



Der ePA-Hack

- **CCC, Chaos-Computer-Club** dringt erfolgreich in die Telematik-Infrastruktur 2024 ein, was zum Stopp der Einführung zum 1.Januar 2025 führte.
- Der bundesweite Rollout wurde auf den 29.April 2025 verschoben.
- Die Einführung Zunächst freiwillig
- Ab dem 1. Oktober 2025 wird die Nutzung der ePA für alle Leistungserbringer bundesweit verpflichtend.

- **Regelungen für Kinder und Jugendliche:**

- Es gibt klare Regelungen, dass Ärzte und Psychotherapeuten bei unter 15-Jährigen keine Daten in die ePA übermitteln müssen, wenn therapeutische Gründe oder das Kindeswohl dem entgegenstehen.

Der Angriff
Die Angriffe waren deshalb erfolgreich, weil sie nicht primär hochkomplexe Software-Schwachstellen ausnutzten, sondern die **schwachen, oft analogen Prozesse zur Identitätsprüfung**, die dem digitalen System vorgelagert sind.

Hier sind die beiden Methoden im Detail erklärt:

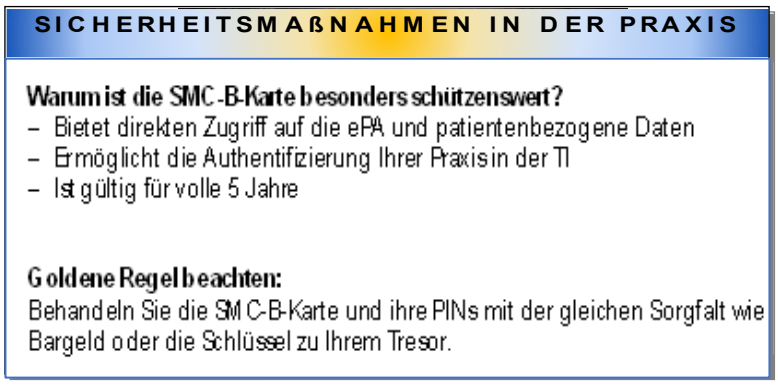
1. Die Methode "Falscher Arzt"
Ziel dieses Angriffs war es, einen offiziellen **elektronischen Heilberufsausweis (eHBA)** zu erhalten, der als digitaler Generalschlüssel für Ärzte im Gesundheitssystem dient.
Fiktive Identität erschaffen: Der Sicherheitsexperte erfand einen Arzt mit Namen, Geburtsdatum und einer Praxisadresse.
Approbationsurkunde fälschen: Er erstellte am Computer eine gefälschte Approbationsurkunde (die offizielle Urkunde zur Zulassung als Arzt). Vorlagen und offizielle Siegel von Universitäten und Behörden sind oft online zu finden, was die Fälschung erleichterte.
Antrag stellen: Mit dieser gefälschten Urkunde beantragte er bei einer der offiziellen Ausgabestellen einen eHBA.
Verifizierungsprozess aushebeln: Der entscheidende Schwachpunkt war, dass die Prüfung damals nicht gegen ein zentrales, digitales Register aller zugelassenen Ärzte erfolgte. Die Sachbearbeiter prüften im Wesentlichen nur, ob das eingereichte Papierdokument echt *aussah*. Da die Fälschung gut gemacht war, wurde sie akzeptiert.

Ergebnis: Der Experte erhielt einen voll funktionsfähigen, gültigen eHBA per Post an seine fiktive Praxisadresse. Mit diesem Ausweis wurde eine SMC-B Karte samt Konnektor bestellt und erhalten. Damit hätte er sich in die Telematik-Infrastruktur als Arzt authentifizieren und potenziell auf die ePA von Patienten zugreifen können.

Die Kernschwachstelle war also die fehlerhaften Ausgabe-Prozesse zur digitalen Gegenprüfung der analogen (und fälschbaren) Papierurkunden beim zentralen Arztregister und die Physische Identitäts-Prüfung bei der Lieferung von Konnektor und SMC-B Karte.
Es wurden also nicht IT-Strukturen gehackt, sondern es ging darum die fehlende Sicherheit in der gesamten Lieferkette und den Betriebsabläufen der TI-Komponenten zu beweisen.

2. Die Methode "Falscher Patient"
Ziel dieses Angriffs war es, die Kontrolle über die ePA einer realen Person zu erlangen.
Öffentliche Daten nutzen: Die Experten wählten eine Person des öffentlichen Lebens und sammelten deren frei verfügbare Daten (Name, Geburtsdatum etc.).
Krankenkasse kontaktieren: Sie riefen bei der Krankenkasse des Opfers an, gaben sich als die Person aus und meldeten die **Gesundheitskarte (eGK) als verloren**. Gleichzeitig gaben sie eine **neue, geänderte Postadresse** an.
Identitätsprüfung umgehen: Die Identitätsprüfung am Telefon oder im Online-Portal der Kasse war zu schwach. Sicherheitsfragen (z.B. "Wie lautet Ihr Geburtsdatum?") konnten mit den öffentlich recherchierten Daten leicht beantwortet werden. Die Adressänderung wurde ohne weitere robuste Prüfung akzeptiert.
Neue Karte und PIN abfangen: Die Krankenkasse schickte daraufhin eine neue, gültige Gesundheitskarte sowie den separaten Brief mit der PIN für die ePA-Nutzung an die vom Angreifer kontrollierte Adresse.
Ergebnis: Mit der neuen Karte und der PIN konnten die Experten die ePA-App der Krankenkasse installieren, den Registrierungsprozess im Namen des Opfers abschließen und hatten somit die volle Kontrolle über dessen (zu dem Zeitpunkt noch leere) e-Patientenakte.

Auch hier war Kernschwachstelle der unsichere Service-Prozess der Krankenkasse, der es zuließ, die Identität einer Person ohne starke Authentifizierung zu übernehmen und deren physische "Schlüssel" (die eGK) umzuleiten.
Beide Fälle zeigen, dass die Sicherheit eines digitalen Systems nur so stark ist wie ihr schwächstes Glied – und das sind oft die menschlichen und administrativen Prozesse an den Schnittstellen. Oder der klassische und alltägliche Konflikt zwischen **Sicherheit und Bequemlichkeit.**

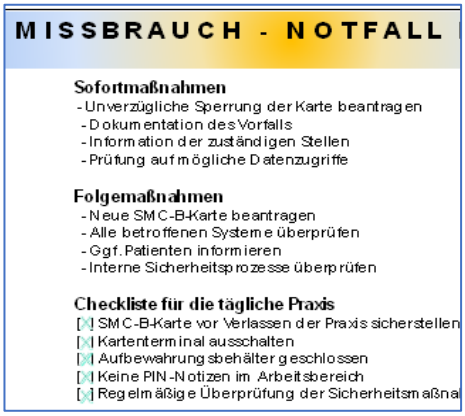


Sicherheitsmaßnahmen

Warum ist die SMC-B-Karte mit Pin-Nummer besonders schützenswert?

- Enthält sensible Verschlüsselungszertifikate (ECC und RSA)
- Bietet direkten Zugriff auf die ePA und patientenbezogene Daten
- Ermöglicht die Authentifizierung Ihrer Praxis in der TI
- Ist gültig für volle 5 Jahre

Die goldene Regel lautet: Behandeln Sie die SMC-B-Karte und ihre PINs mit der gleichen Sorgfalt wie Bargeld oder die Schlüssel zu Ihrem Tresor. **Die physische Karte und das Wissen um die PIN dürfen niemals zusammen in die falschen Hände geraten.**



Sofortmaßnahmen:

- Unverzügliche Sperrung der Karte beantragen
- Dokumentation des Vorfalls
- Information der zuständigen Stellen
- Prüfung auf mögliche Datenzugriffe

Folgemaßnahmen:

- Neue SMC-B-Karte beantragen
- Alle betroffenen Systeme überprüfen
- Ggf. Patienten informieren
- Interne Sicherheitsprozesse überprüfen

Checkliste für die tägliche Praxis

[ ] SMC-B-Karte vor Verlassen der Praxis sicherstellen
[ ] Kartenterminal ausschalten
[ ] Aufbewahrungsbehälter verschließen
[ ] Keine PIN-Notizen im Arbeitsbereich
[ ] Regelmäßige Überprüfung der Sicherheitsmaßnahmen

Die 5 Goldenen Regeln des Datenschutzes

Genauso wenig wie man Patientenakten nicht offen herumliegen lassen darf, müssen digitale Daten vor dem Zugriff aus dem Internet oder vor neugierigen Blicken auf einen Monitor mit früheren Patientendaten geschützt werden.

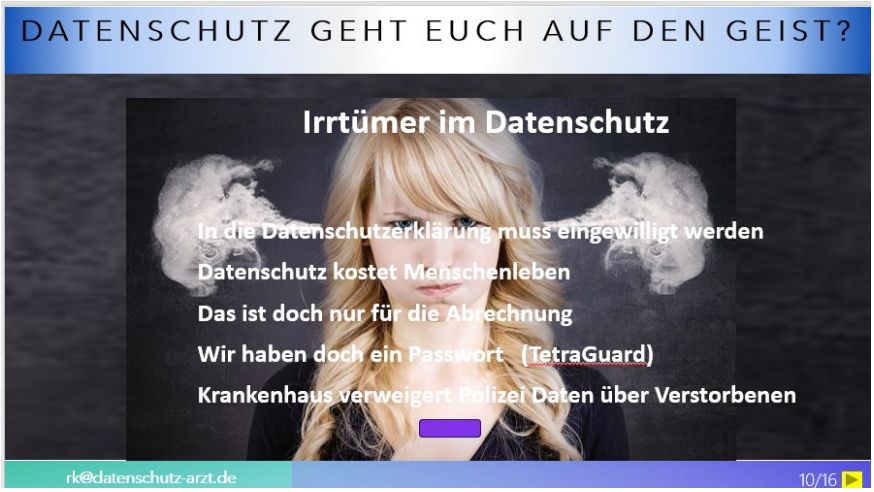
Das sind die Grundsätze im Datenschutz mit seinen wichtigsten Regeln:

1. Rechtmäßigkeit

Bevor Sie Daten verarbeiten, brauchen Sie dazu eine Erlaubnis. Die Rechtsgrundlage muss aus Art. 6 DSGVO stammen. Beispiele sind:

- **Patienten-Einwilligung** (Art. 6 Abs. 1 lit. a DSGVO)
- **gesetzliche Grundlage** (Art. 6 Abs. 1 lit. c DSGVO), z. B. gesetzliche Dokumentationspflichten
- **Behandlungsvertrag** (Art. 6 Abs. 1 lit. b DSGVO)
- **Notfallsituation** (Art. 6 Abs. 1 lit. d DSGVO): wenn die Datenverarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Ohne eine solche Rechtsgrundlage dürfen keine Daten gespeichert oder weitergegeben werden.

2. **Transparenz**
   - Patienten müssen wissen, was mit ihren Daten passiert
   - Vor Verarbeitung muss er mit der Datenschutz-Patienteninformation informiert werden
   - Patienten-Information an der Anmeldung
   - Datenschutzerklärung auf der Webseite
   - Ähnlich wie Sie Patienten über Behandlungsmethoden aufklären
   - Alle Datenverarbeitungen müssen nachvollziehbar sein
3. **Datenminimierung**
   - Nur solche Daten sammeln, die wirklich nötig sind
   - So wie Sie in der Patientenkarte nur relevante Informationen notieren
   - Keine Spekulation oder "für alle Fälle“
4. **Sicherheit**
   - Daten müssen geschützt werden wie wertvolle Medikamente
   - Datenschutz-Dokumentation, (Verfahrensverzeichnis, Technische und Organisatorische Maßnahmen)
   - Passwörter und Zugangsregeln beachten
   - Regelmäßige Updates und Backups wie bei der Praxis-Software
5. **Verantwortlichkeit**
   - Jeder muss für die Daten verantwortlich sein
   - Regelmäßige Sensibilisierung und Schulung
   - Wie Sie sich um Ihre Patientenakten kümmern
   - Fehler melden und korrigieren, wenn etwas schiefläuft



Irrtümer im Datenschutz

In die Datenschutzerklärung muss eingewilligt werden?

Hierbei ist Folgendes zu bedenken: Bei der Datenschutzerklärung handelt es sich nicht um einen Vertrag. Wie auch schon die Datenschutzkonferenz erklärt hat, informiert die Datenschutzerklärung nach Art. 13 DSGVO lediglich betroffene Personen u.a. darüber, zu welchem Zweck und auf welcher Rechtsgrundlage ihre Daten wie verarbeitet und welche Betroffenenrechte bestehen. Webseitenbesucher können diese Informationen z.B. durch eine Verlinkung auf die Datenschutzbestimmungen zur Kenntnis nehmen und dies ggf. durch einen Klick dokumentieren. Dadurch wird die Kenntnisnahme aber noch keine erteilte Einwilligung nach Art. 7 DSGVO.

Denn die Datenschutzhinweise stehen nicht zur Disposition. Sie sind nicht verhandelbar. Ob der Websitebesucher die Datenschutzhinwiese also zusätzlich akzeptiert, spielt keine Rolle für die Erfüllung der Informationspflicht des Arztes. Der so häufig auf Webseiten gelesene Satz beim

Absenden eines Kontaktformulars o.ä. *„Ich akzeptiere die Datenschutzerklärung“,* vermischt Informationspflicht und Einwilligung.

Die Einholung einer Einwilligung (und u.U. sogar auch die Bestätigung der Kenntnisnahme) können nach Ansicht des Obersten Gerichtshofs in Österreich (OGH) und des europäischen Datenschutzausschusses (EDSA) letztlich gegen den Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO) verstoßen. Das Kammergericht urteilte in diesem Zusammenhang, dass zustimmungsbedürftige Datenschutzbestimmungen wegen Unvereinbarkeit mit den Grundgedanken der DSGVO als AGB-rechtliche Verstöße zu werten seien.

Datenschutz kostet Menschenleben?

Die Aussage "Datenschutz kostet Menschenleben" ist ein Paradebeispiel für Unwissen im Datenschutzkontext, da sie:

- Vereinfachend und irreführend ist: Sie reduziert ein komplexes Thema auf eine einfache, aber falsche Gegenüberstellung. Datenschutz und Menschenleben sind keine Gegensätze, sondern können und müssen miteinander vereinbart werden.
- Panikmache: Sie schürt Angst und Unsicherheit, indem sie suggeriert, dass Datenschutz zwangsläufig zu Todesfällen führt.
- Von Verantwortlichkeit ablenkt: Sie dient oft als Ausrede, um notwendige Datenschutzmaßnahmen zu umgehen oder zu vernachlässigen.
- Die Bedeutung des Datenschutzes missachtet: Sie ignoriert die grundlegenden Rechte und Freiheiten, die durch den Datenschutz geschützt werden.

Das ist doch nur für die Abrechnung?

Beispiel:

- Eine Arztpraxis speichert unnötig viele Patientendaten in der Praxisverwaltungs-Software, da sie glauben, dass es für mögliche künftige Dinge notwendig sein könnte.

Problem, fragen Sie sich, sind die Daten…

- für die Behandlung erforderlich?
- für die Abrechnung nötig?
- entspricht es den gesetzlichen Vorgaben?
- Die sogenannte Datensparsamkeit ist ein Grundprinzip des Datenschutzes.

Wir haben doch ein Passwort!

Beispiel:

- Eine Arztpraxis speichert Patientendaten unverschlüsselt auf einem Computer, der nur durch ein einfaches Passwort geschützt ist.

Problem:

- Ein einfaches Passwort bietet keinen ausreichenden Schutz vor unbefugtem Zugriff.
- Medizinische Daten müssen durch angemessene technische und organisatorische Maßnahmen geschützt werden.
- Dazu gehören starke Passwörter, Verschlüsselung und regelmäßige Sicherheitsupdates.
- Ein Passwort alleine reicht nicht aus, um die Anforderungen der DSGVO zu erfüllen.
- Der Sicherheitsanbieter TetraGuard bietet als einziges Unternehmen Datenbankverschlüsselung an!

Krankenhaus verweigert Polizei Informationen über einen verstorbenen Patienten „Datenschutz“.

Der Fall:

In der Ebersberge Klinik verstirbt ein Mann. Da keine Verwandten bekannt sind, wird er vorerst in der Leichenhalle des KH eingelagert.

Mittlerweile vermissen aber Verwandte diesen Mann und geben eine Vermisstenanzeige bei der Polizei auf.

Routine mäßig checken die Beamten auch alle umliegenden Krankenhäuser ab.

Vom KH-Ebersberg erhalten Sie die Auskunft, der Mann sei entlassen worden und weitere Auskünfte könnten aus Datenschutz rechtlichen Gründen nicht gegeben werden.
Erst nach vielen Tagen fällt das Missverständnis auf und als Ausrede wird vom KH nachgereicht: „Am Telefon könne man einen Anrufer (Polizei) nicht identifizieren und gebe daher keine Auskunft.

Problem:
Das Verhalten des Krankenhauses in diesem Fall wirft eine Reihe von rechtlichen Fragen auf und kann mehrere Rechtsverletzungen darstellen. Hier sind die wichtigsten Aspekte:

a) Verletzung der Informationspflichten:

Falsche Auskunft:

- Die falsche Auskunft, dass die Person entlassen wurde, stellt eine Verletzung der Informationspflichten dar. Krankenhäuser haben im Rahmen ihrer Organisation sicherzustellen, dass Auskünfte korrekt und vollständig erteilt werden.
- Dies gilt insbesondere gegenüber Behörden wie der Polizei, die im Rahmen ihrer Aufgaben auf korrekte Informationen angewiesen sind.
- Verweigerung der Auskunft:
- Die pauschale Verweigerung der Auskunft unter Berufung auf den Datenschutz ist in dieser Form nicht zulässig. Wie bereits erörtert, gibt es rechtliche Grundlagen, die der Polizei in bestimmten Fällen ein Auskunftsrecht einräumen.
- Eine sachgerechte Abwägung zwischen Datenschutz und den berechtigten Interessen der Polizei hätte erfolgen müssen.

b) Verletzung des Datenschutzes:

Fehlerhafte Identifizierung:

- Die Erklärung des Krankenhauses, eine Identifizierung am Telefon sei schwierig, wirft Fragen nach den internen Prozessen auf.
- Krankenhäuser sind verpflichtet, angemessene Maßnahmen zu ergreifen, um die Identität von Personen sicherzustellen und unbefugte Auskünfte zu vermeiden.
- Wenn die Identifizierung am Telefon als problematisch bekannt ist, hätten alternative Verfahren etabliert werden müssen.
- Unangemessene Berufung auf den Datenschutz:
- Der Datenschutz darf nicht als pauschale Begründung für die Verweigerung von Auskünften gegenüber berechtigten Stellen missbraucht werden.
- Es ist erforderlich, im Einzelfall eine Abwägung zwischen den Datenschutzrechten des Patienten und den berechtigten Interessen Dritter vorzunehmen.

c) Mögliche weitere rechtliche Konsequenzen:

Behinderung von Ermittlungen:

- Die falsche Auskunft und die Verweigerung der Auskunft könnten als Behinderung von Ermittlungen im Sinne des Strafprozessrechts gewertet werden.

Zivilrechtliche Ansprüche:

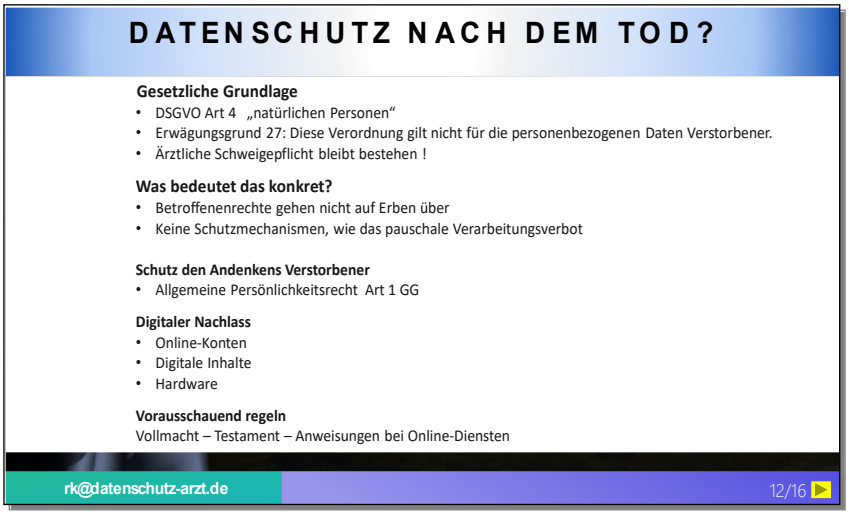
- Die Angehörigen des Verstorbenen könnten zivilrechtliche Ansprüche gegen das Krankenhaus geltend machen, wenn ihnen durch die fehlerhafte Auskunft ein Schaden entstanden ist.

Datenschutzrechtliche Konsequenzen:

- Die zuständige Datenschutzbehörde könnte ein Verfahren gegen das Krankenhaus einleiten und Bußgelder verhängen.

Zusammenfassend:

Das Krankenhaus hat durch die falsche Auskunft und die unangemessene Verweigerung der Auskunft mehrere Rechtsverletzungen begangen. Es ist wichtig, dass Krankenhäuser ihre internen Prozesse überprüfen und sicherstellen, dass sie ihren Informationspflichten und den Anforderungen des Datenschutzes gerecht werden.



Datenschutz nach dem Tod

Was passiert eigentlich mit personenbezogenen Daten, wenn jemand stirbt? Welche Rechte gibt es hinsichtlich personenbezogener Daten nach dem Tod? Was sollten Angehörige beachten? Welche Möglichkeiten gibt es, Daten über den Tod hinaus zu schützen oder zu bewahren? Dieser Beitrag soll ein paar Wegweiser geben, wie es mit dem Recht und den Daten nach dem Tod weiter geht.

Die gesetzliche Grundlage

Die rechtliche Grundlage ist immer zunächst im Gesetz zu suchen. In der Definition der personenbezogenen Daten wird nur von „natürlichen Personen“ (Art. 4 Nr. 1 DSGVO) gesprochen.

Der Blick in die Erwägungsgründe schafft Klarheit: In Erwägungsgrund 27 werden Daten Verstorbener explizit von der Geltung der DSGVO ausgenommen.

„Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener.“

Nur in Spezialgesetzen finden sich vereinzelte Vorschriften. Insbesondere § 203 Abs. 4 Nr. 3 StGB regelt, dass fremde Geheimnisse von Verstorbenen nicht offenbart werden dürfen, sofern diese in einem besonderen Vertrauensverhältnis offenbart wurden. Dies umfasst auch Geheimnisse, die Datenschutzbeauftragte in ihrer Tätigkeit erfahren haben.

Für die Sozialgesetzgebung regelt § 35 Abs. 5 SGB I, dass Sozialdaten Verstorbener entsprechend der Vorschriften in SGB X für Verwaltungsverfahren verarbeitet werden dürfen. Für die Steuerverwaltung gilt ähnliches nach § 2a Abs. 5 Nr. 1 AO.

Was bedeutet das konkret?

Die wichtigste Konsequenz daraus, dass die DSGVO nicht für Daten Verstorbener gilt, ist das insbesondere die

Betroffenenrechte nicht auf die Erben übergehen. Gleichzeitig entfallen aber auch andere Schutzmechanismen, wie das pauschale Verarbeitungsverbot.

Verantwortliche können mit den Daten Verstorbener aber wenig anfangen. Verstorbene können keine neuen Verträge eingehen, und hinsichtlich der Erben ist eine eigene Rechtsgrundlage für die Verarbeitung von Daten erforderlich, da diese natürlichen Personen sind. Viele Datenverarbeitungen von Daten Verstorbener laufen faktisch ins Leere, nur statistische Erhebungen und ggf. medizinische Auswertungen könnten von der Verarbeitung profitieren. Allerdings müssen hierfür die Daten meist schon vor dem Tod der Person mit einer Rechtsgrundlage erhoben worden sein. Denn auch hier kann die verstorbene Person keine Informationen mehr geben.

Schutz den Andenkens Verstorbener außerhalb des Datenschutzes

Neben den Regelungen zur Verarbeitung personenbezogener Daten gibt es aber andere Gesetze, die das Andenken Verstorbener schützen.

Das Allgemeine Persönlichkeitsrecht leitet sich in Deutschland aus Artikel 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG her. Dieses gilt nach der Rechtsprechung des BGH, allein hergeleitet aus Art. 1 GG, über den Tod hinaus. Das postmortale Persönlichkeitsrecht, die ärztliche Schweigepflicht und das BGB bilden ein komplexes Geflecht, das die Handhabung von Daten Verstorbener regelt. Die Abwägung zwischen dem Interesse der Erben an den Daten und dem Schutz der Privatsphäre des Verstorbenen ist oft eine Herausforderung. Die Gesetzeslage ist hier in Deutschland nicht eindeutig geregelt, und muss meistens in einer

Einzelfallentscheidung geprüft werden. Je mehr das Andenken des Verstorbenen aber verblasst, desto schwächer wird auch der postmortale Persönlichkeitsschutz. Daraus ergibt sich eine Art „Verfallsdatum“, das aber nur in einzelnen Spezialgesetzen auf eine feste Zeit reduziert wird. In der Rechtsprechung waren daher 10-30 Jahre in verschiedenen Konstellationen als angemessen betrachtet worden.

Digitaler Nachlass

Für die Praxis ist zudem relevant, wie mit den Datenspuren gerade im Internet umgegangen werden soll. Seit einem Urteil des BGH 2018 ist geklärt, dass die vertraglichen Rechte und Pflichten an einem Social Media-Account auch Teil des Erbes sind und an den oder die Erben übergehen. Insofern sind die Anbieter verpflichtet, den Erben Zugang zu verschaffen.

Gerade in der Zeit direkt nach dem Tod ist es für die Angehörigen aber oft relevant, bereits schnell Zugriff auf Konten zu erhalten, um zu erfahren, ob es laufende Verträge oder offene Rechnungen gibt. Auch im Hinblick darauf, ob ein Erbe überhaupt angenommen oder ausgeschlagen werden soll, ist eine Übersicht über die ggf. digital geschlossenen Verträge sehr hilfreich. Dafür kann man nicht warten, bis man als Erbe mit Erbschein ausgestattet ist – denn dafür muss das Erbe angenommen werden, und dann gibt es kein Zurück mehr.

Hier helfen aber die gesetzlichen Vorschriften alle nicht weiter. Auskunftsrechte des Betroffenen stehen den Angehörigen nicht zu. Sonderregelungen hat der Nachlass im Datenschutzrecht keine. Wer sicher gehen möchte, dass die Angehörigen den Nachlass auch in dieser Hinsicht gut regeln können, wird seine Passwörter für die Hinterbliebenen hinterlegen müssen. Wie das in der Praxis dann sicher zu bewerkstelligen ist, hängt auch vom Vertrauensverhältnis zu den Angehörigen und den technischen und räumlichen Möglichkeiten ab.

Online-Konten: E-Mail-Konten (z. B. Gmail, Outlook)

- Social-Media-Profile (z. B. Facebook, Instagram, Twitter)
- Online-Banking-Konten
- Online-Shopping-Konten (z. B. Amazon, eBay)
- Streaming-Dienste (z. B. Netflix, Spotify)
- Cloud-Speicher (z. B. Google Drive, Dropbox)
- Kryptowährung-Wallets

Digitale Inhalte:

- Fotos und Videos
- Dokumente und Dateien
- Musik und Filme
- Websites und Blogs

Hardware:

- Computer und Laptops
- Smartphones und Tablets
- Externe Festplatten und USB-Sticks

Vorausschauend regeln:

Um den Zugriff auf den digitalen Nachlass zu ermöglichen, sollten Verstorbene zu Lebzeiten Vorkehrungen treffen:

Vollmacht:

- Eine Vollmacht kann einer Vertrauensperson den Zugriff auf bestimmte Online-Konten und Daten ermöglichen.

Testament:

- Im Testament können Anweisungen zur Verwaltung und Löschung von Online-Konten sowie zur Weitergabe von digitalen Inhalten festgehalten werden.
- Eine Liste von Passwörtern und Zugangsdaten kann erstellt werden, diese Liste sollte sicher verwahrt werden.

Anweisungen bei Online-Diensten:

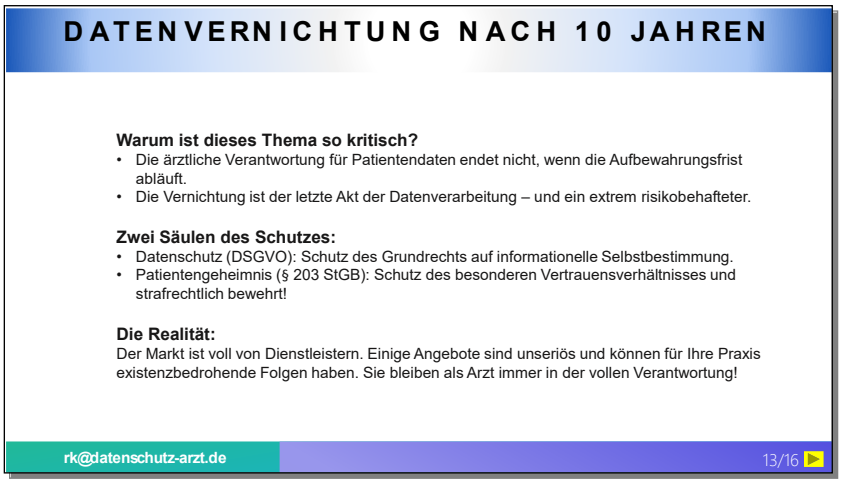
- Viele Online-Dienste bieten Optionen zur Verwaltung des Kontos im Todesfall an (z. B. Facebooks "Nachlasskontakt").

Rechtliche Aspekte:

- Der Bundesgerichtshof hat entschieden, dass der digitale Nachlass Teil des Erbes ist.
- Erben haben grundsätzlich das Recht, auf die digitalen Daten des Verstorbenen zuzugreifen.
- Datenschutzrechtliche Bestimmungen müssen beachtet werden, insbesondere bei der Weitergabe von personenbezogenen Daten.

Empfehlungen:

- Erben sollten sich einen Überblick über die Online-Aktivitäten des Verstorbenen verschaffen.
- Sie sollten sich an die jeweiligen Anbieter wenden, um den Zugriff auf die Konten zu regeln.
- Bei Unsicherheiten sollten sie rechtlichen Rat einholen.

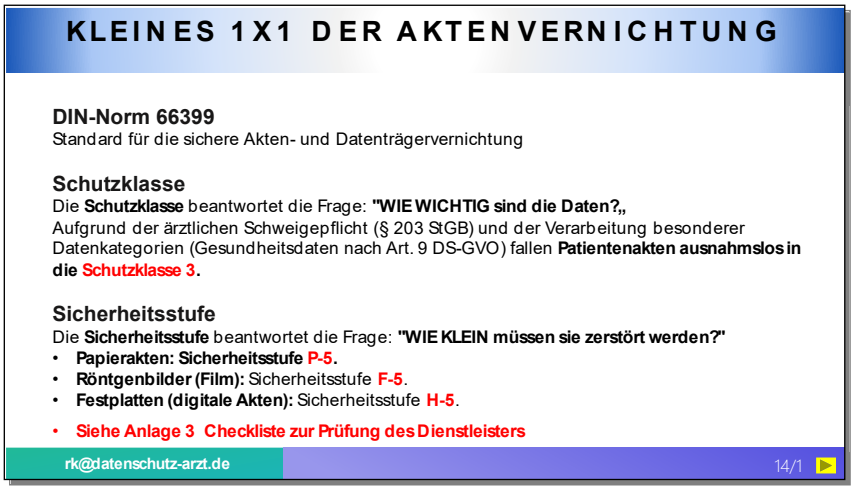


Warum ist dieses Thema so kritisch?

- Die ärztliche Verantwortung für Patientendaten endet nicht, wenn die Aufbewahrungsfrist abläuft.
- Die Vernichtung ist der letzte Akt der Datenverarbeitung – und ein extrem risikobehafteter.

Zwei Säulen des Schutzes:

- Datenschutz (DSGVO): Schutz des Grundrechts auf informationelle Selbstbestimmung.
- Patientengeheimnis (§ 203 StGB): Schutz des besonderen Vertrauensverhältnisses und strafrechtlich bewehrt!



Kleines 1x1 der Aktenvernichtung
Die Realität:
Der Markt ist voll von Dienstleistern. Viele Angebote sind unseriös und können für die Arzt-Praxis existenzbedrohende Folgen haben. Sie bleiben als Arzt immer in der vollen Verantwortung!

In der Anlage erhalten Sie eine Checkliste mit der Sie das Angebot eines Aktenvernichter-Lieferanten überprüfen können.

Oder Empfehlung ist, diese Checkliste zuzuschicken, um langwierige Diskussionen zu verkürzen oder falsche Angebote zu blocken.

Die DIN-Norm 66399, ist der Standard für die sichere Akten- und Datenträgervernichtung.
Die **Schutzklasse** beantwortet die Frage: **"WIE WICHTIG sind die Daten?"**
Die **Sicherheitsstufe** beantwortet die Frage: **"WIE KLEIN müssen sie zerstört werden?"**

Hier ist die detaillierte Erklärung:
Die Schutzklasse: Die Einstufung der Daten (Das "WARUM")
Die Schutzklasse stuft die **Daten selbst** nach ihrer Sensibilität und dem potenziellen Schaden ein, der bei einer unbefugten Offenlegung entstehen würde. Sie treffen diese Einstufung als Arztpraxis, bevor Sie die Daten zur Vernichtung geben.
Es gibt drei Schutzklassen:

Schutzklasse 1 (Normaler Schutzbedarf):

Daten: Interne Informationen, deren unbefugte Kenntnisnahme begrenzte negative Auswirkungen hätte.

Beispiele: Allgemeine Korrespondenz (ohne sensible Daten), Kataloge, Werbematerial.

Schutzklasse 2 (Hoher Schutzbedarf):

Daten: Vertrauliche Informationen, deren Offenlegung erhebliche negative Folgen für Betroffene oder gegen Gesetze verstoßen würde.

Beispiele: Personalakten, Finanzdaten, Angebote, Bilanzen.

Schutzklasse 3 (Sehr hoher Schutzbedarf):

Daten: Geheime und existenzkritische Informationen, deren Offenlegung eine Gefahr für Leib und Leben, die persönliche Freiheit oder Berufsgeheimnisse darstellen würde.

Beispiele: Patientenakten, geheime Forschungsdaten, Prozessakten, Daten von Geheimdiensten.

Für die Arztpraxis ist die Sache eindeutig: Aufgrund der ärztlichen Schweigepflicht (§ 203 StGB) und der Verarbeitung besonderer Datenkategorien (Gesundheitsdaten nach Art. 9 DS-GVO) fallen **Patientenakten ausnahmslos in die Schutzklasse 3.**

Die Sicherheitsstufe: Die Methode der Vernichtung (Das "WIE")

Die Sicherheitsstufe ist die **technische Anforderung** an den Zerstörungsprozess. Sie leitet sich aus der Schutzklasse ab und definiert, wie klein die Partikel nach der Vernichtung maximal sein dürfen. Die DIN 66399 definiert sieben Sicherheitsstufen für verschiedene Materialarten (gekennzeichnet durch Buchstaben, z.B. **P** für Papier, **F** für Film/Röntgenbilder, **H** für Festplatten).

Hier die relevanten Stufen für Papier (P):

P-1 bis P-3: Grobe bis feine Streifen. Für allgemeine bis vertrauliche Dokumente (Schutzklasse 1 und 2). **Für Patientenakten ungeeignet.**

P-4 (Partikelschnitt): Max. Partikelfläche 160 mm^2. Gilt als Mindestanforderung für viele sensible Daten.

P-5 (Partikelschnitt): Max. Partikelfläche 30 mm^2. **Dies ist die empfohlene Stufe für Daten der Schutzklasse 3, wie z.B. Patientenakten.** Eine Rekonstruktion ist nur mit speziellem Laboraufwand denkbar.

P-6 und P-7: Extrem feiner Partikelschnitt (Staub). Für Hochsicherheits- und Geheimdienst-Dokumente.

Zusammenhang und Fazit

Aus der Schutzklasse leitet sich die erforderliche Sicherheitsstufe ab.

Wenn Sie als Arztpraxis festlegen, dass Ihre Akten **Schutzklasse 3** haben (was sie immer tun müssen), müssen Sie zwingend einen Vernichtungsprozess wählen, der eine entsprechend hohe **Sicherheitsstufe** garantiert.

Für Ihre Patientenakten bedeutet das:

Papierakten: Mindestens Sicherheitsstufe **P-4**, dringend empfohlen ist **P-5**.
Röntgenbilder (Film): Mindestens Sicherheitsstufe **F-4**, empfohlen ist **F-5**.
Festplatten (digitale Akten): Mindestens Sicherheitsstufe **H-5**.
Kurz gesagt: Die **Schutzklasse** ist Ihre strategische Entscheidung über den Wert der Daten, die **Sicherheitsstufe** ist die technische Ausführung, um diesen Wert zu schützen.

Was heißt **„empfohlen“**:
Die Antwort liegt im Unterschied zwischen **"ausreichend"** und **"angemessen"** und vor allem im **Haftungsrisiko im Schadensfall**.

Der "Stand der Technik" nach DS-GVO

Artikel 32 der DS-GVO verlangt Schutzmaßnahmen nach dem "Stand der Technik". Dieser Begriff ist dynamisch und entwickelt sich weiter. Für normale Geschäftsdaten mag P-4 heute der Stand der Technik sein. Für besondere Datenkategorien (Gesundheitsdaten) und Berufsgeheimnisse

argumentieren viele Juristen und Datenschützer, dass eine höhere Stufe wie P-5 dem angemessenen "Stand der Technik" entspricht. Mit P-5 sind Sie also zukunftssicherer.

Das technische Restrisiko

Der Aufwand zur Rekonstruktion von Daten aus P-4-Partikeln ist hoch, aber mit krimineller Energie und spezieller Software nicht unmöglich. Bei P-5-Partikeln ist eine Rekonstruktion praktisch ausgeschlossen. Bei Patientendaten sollte das Ziel sein, das Restrisiko so weit wie technisch und wirtschaftlich vertretbar zu minimieren.