1. Der Umstieg auf Windows 11 – Sicherheit, Zwang und Zukunftsstrategie

Dieses Thema sorgt aktuell für viel Gesprächsstoff – nicht zuletzt, weil der offizielle Support von Windows 10 im Oktober 2025 endet. Und genau dieser Umstand wird von manchen IT-Dienstleistern als **künstlicher Zwang** genutzt, um uns mit **überzogenen, überstürzten und viel zu teuren Hardware-Angeboten** unter Druck zu setzen.

Mein Ziel heute ist es, Ihnen die Fakten zu liefern, damit wir gemeinsam einen **ruhigen, sicheren und wirtschaftlichen Fahrplan** für unsere Praxis festlegen können. Wir werden sehen: Es gibt keinen Grund zur Panik.

1.1. Der wahre Grund für neue Hardware: Moderne Sicherheit

Zunächst die Fakten: Der Umstieg auf Windows 11 ist keine Laune von Microsoft, sondern dient primär der **verbesserten Systemsicherheit**. Hier liegt der Unterschied zu Windows 10, und hier liegt auch der Grund, warum viele unserer aktuellen PCs die Anforderungen nicht erfüllen.

Der zentrale Punkt ist das **Trusted Platform Module 2.0 – kurz TPM 2.0.**

- **Was ist TPM 2.0?** Es ist ein **spezieller Kryptochip** auf dem Mainboard, der wie ein **Hardware-Tresor** funktioniert. Er speichert kryptografische Schlüssel und prüft die Integrität unserer System-Firmware, bevor das Betriebssystem überhaupt startet.
- **Der Nutzen:** TPM 2.0 ist die Grundlage für wesentliche Sicherheitsfunktionen wie die hardwarebasierte Verschlüsselung (z.B. BitLocker) und **Secure Boot**, das sicherstellt, dass beim Start nur vertrauenswürdige Software geladen wird.

Fazit: Ja, langfristig ist ein Wechsel zu Windows 11-kompatibler Hardware notwendig, um das höchste Sicherheitsniveau – *Security by Design* – für unsere sensiblen Daten zu erreichen. **Aber:** Wir lassen uns nicht unter Druck setzen.

1.2. Die Lösung für die Übergangszeit: Das ESU-Programm

Der offizielle Support für Windows 10 endet im Oktober 2025. Nach diesem Datum würden wir regulär keine Sicherheitsupdates mehr erhalten. **Das klingt dramatisch, ist es aber nicht.**

Microsoft hat mit dem **Extended Security Updates (ESU)-Programm** eine offizielle und sichere Übergangslösung geschaffen, die uns Luft verschafft.

Das ESU-Programm für Windows 10:

- **Was es leistet:** ESU verlängert den Support für Windows 10 um **maximal drei Jahre** (bis Oktober 2028). In dieser Zeit erhalten wir weiterhin monatliche Sicherheitsupdates für alle als **"kritisch" oder "wichtig"** eingestuften Sicherheitslücken.
- **Die Kosten in der Praxis:** Die Kosten beginnen derzeit bei ca. **60 bis 80 Euro (netto) pro Gerät und Jahr** für die ersten 12 Monate.
- **Der Mehrwert:** Für diese überschaubaren Kosten erkaufen wir uns **wertvolle Zeit** – Zeit, um die notwendige Hardware in Ruhe zu beschaffen, unsere Fachanwendungen zu prüfen und die Migration ohne Stress durchzuführen.

1.3. Sicherheit in der Arztpraxis: Warum ESU ausreicht

Die entscheidende Frage lautet: **Reicht dieser verlängerte Schutz durch das ESU-Programm für eine Arztpraxis, die mit Patientendaten arbeitet, aus?**

Die klare Antwort ist: Ja, er reicht für die Übergangszeit.

- **Erfüllung der VIA-Ziele (Vertraulichkeit, Integrität, Verfügbarkeit):** Das ESU-Programm liefert genau die Updates, die notwendig sind, um Angriffe über die wichtigsten und bekanntesten Sicherheitslücken zu verhindern. Solange Microsoft kritische Lücken schließt, erfüllen wir unsere Pflicht, den **Stand der Technik** zur Abwehr von Gefahren zu gewährleisten.
- **Verteidigung in der Tiefe:** Unsere Sicherheit hängt nicht allein vom Betriebssystem ab. Unsere **Firewall**, unsere **Anti-Viren-Software** und die **hochgesicherte Telematikinfrastruktur (TI)** bilden zusätzliche Schutzebenen. Das ESU-Programm schließt lediglich die Lücke, die im Oktober 2025 entstehen würde.

1.4. Strategische Alternative: Der Wechsel zur Cloud (Managed Service Provider)

Anstatt den Hardware-Zwang alle paar Jahre neu zu durchleben, sollten wir diese Situation nutzen, um eine **strategische Alternative** zu prüfen: **Die Migration unserer Praxis-IT in die Cloud zu einem Managed Service Provider (MSP).**

Vorteile eines MSP und der Cloud-Betrieb:

- **Vorteile eines MSP:** Ein MSP übernimmt die **komplette IT-Verantwortung**. Er garantiert, dass das Betriebssystem (**Windows 11**) und alle Server immer aktuell, gewartet und konform sind – **ohne dass wir uns kümmern müssen.**
- **Vorteile für die Praxis:**
  - **Entlastung:** Wir müssen uns nicht mehr um IT-Probleme kümmern, sondern können uns auf unsere medizinische Kernkompetenz konzentrieren.
  - **Planbarkeit:** Hohe Investitionskosten (**CAPEX**) werden in planbare, monatliche Betriebskosten (**OPEX**) umgewandelt.

Kostenvergleich auf 10 Jahre: Lokale IT versus Cloud

Hier müssen wir die **Gesamtkosten über 10 Jahre** und das Risiko betrachten. Bei lokaler IT haben wir zwei Zyklen von Server- und PC-Neukäufen, unvorhergesehene Reparaturen und ein hohes Risiko bei Cyberangriffen:

Kostenfaktor	Lokale Hardware (10 Jahre)	MSP Cloud-Lösung (10 Jahre)
Hardware-Kosten (Neu)	Sehr hoch (ca. 18.000 € für PCs und Server)	**0 €** (Wir nutzen die alten PCs als Clients)
Datensicherung & Verfügbarkeit	Manuelle, risikobehaftete Backups	**Garantierte Verfügbarkeit** (SLA) und redundante Profi-Sicherungen.
Cyberangriffe/Risiko	**Sehr hoch:** Tragen wir selbst (Ausfall, Datenverlust, Bußgelder).	**Niedrig:** Das IT-Risiko liegt beim spezialisierten MSP in zertifizierten Rechenzentren.

Die Cloud-Lösung bietet uns eine **Versicherungsleistung**: Gegen planbare monatliche Kosten erhalten wir die Garantie für Sicherheit und Verfügbarkeit – ein unschätzbarer Wert in Zeiten steigender Cyberbedrohungen.

1.5. Schlusswort: Die Kontrolle liegt bei uns

Die Umstellung auf Windows 11 zwingt uns, unsere IT neu zu bewerten. Wir nutzen diese Chance:

1. **Kein Stress:** Das **ESU-Programm** sichert uns die nötige Zeit und verhindert überstürzte Kaufentscheidungen.
2. **Strategische Prüfung:** Wir werden die Zeit nutzen, um nicht nur teure Hardware-Angebote, sondern auch **detaillierte Cloud-Angebote von MSPs** einzuholen und die Langzeitkosten transparent zu vergleichen.

Wir behalten die Kontrolle. Wir sichern unsere Praxis ab und investieren klug in unsere Zukunft.

2. Grundlegende Maßnahmen und Handreichungen
Jeder von uns ist täglich mit der Verarbeitung sensibler Patientendaten befasst. Daher ist es essentiell, ein

Verfahrensverzeichnis zu führen, in dem alle Datenverarbeitungsprozesse dokumentiert sind. Dazu gehören die Patientendokumentation, die Abrechnung und auch die Kommunikation mit anderen Stellen wie Jugendämtern oder Schulen. Das Kernstück des Datenschutzes ist dabei die

ärztliche Schweigepflicht (§ 203 StGB).

Ein weiterer grundlegender Aspekt ist die **Einwilligung**. Bei Minderjährigen ist dies besonders komplex. Wir müssen klären, wer einwilligen darf: Die Sorgeberechtigten sind bis zu einem bestimmten Alter die Ansprechpartner, während Jugendliche ab dem 16. Lebensjahr oft als einwilligungsfähig gelten. Dies ist jedoch stets eine Einzelfallentscheidung, die von der geistigen und emotionalen Reife des Jugendlichen abhängt.

---

2. Datenschutz-Grundsätze

2.1. Stellenwert der Gesundheitsdaten im Datenschutz

Gesetzliche Pflichten des Datenverarbeiters

- **Hintergrund:** Gesundheitsdaten, wie Diagnosen oder Befunde, gelten juristisch als **besondere Kategorien personenbezogener Daten**, oft als "sensible Daten" bezeichnet.
- **Warum?** Die Offenlegung dieser Daten kann für Patienten zu Stigmatisierung, Diskriminierung oder Nachteilen führen.
- **Rechtsgrundlage: Art. 9 Abs. 1 DSGVO** untersagt die Verarbeitung dieser Daten grundsätzlich. Die Verarbeitung in der Praxis ist nur wegen der **Gesundheitsvorsorge und Behandlung** zulässig (**Art. 9 Abs. 2 lit. h DSGVO**).

Verantwortlichkeit des Arztes

- **Hintergrund:** Wer trägt im Fall der Fälle die rechtliche Verantwortung?
- **Der Arzt als Verantwortlicher:** Sie, als Inhaber oder ärztlicher Leiter der Praxis, sind der **Verantwortliche** im Sinne des **Art. 4 Nr. 7 DSGVO**.
- **Konsequenz:** Diese Verantwortung ist nicht delegierbar. Sie müssen die Organisation sicherstellen. Wenn ein Mitarbeiter einen Datenschutzfehler macht, sind Sie derjenige, der dafür geradesteht und den Vorfall melden muss.

2.2. Erste Dokumentarische Maßnahmen

Die Einhaltung der Vorschriften muss dokumentiert werden, um im Zweifel nachweisen zu können, dass wir unsere Pflichten erfüllt haben.

Verfahrensverzeichnis (Verzeichnis von Verarbeitungstätigkeiten)

- **Hintergrund:** Das Verfahrensverzeichnis (VvV) ist das **Inventar unserer Datenverarbeitung**. Es ist das Herzstück der Dokumentationspflicht.
- **Inhalt:** Es listet auf, *was* wir mit Patientendaten machen (z.B. "Abrechnung", "Behandlung"), *welche* Daten wir dafür erfassen (Diagnose, Name) und *wie lange* wir sie speichern.
- **Rechtsgrundlage: Art. 30 DSGVO**.
- **Handout:** Muster siehe Anlage (Muster-Verfahrensverzeichnis)

Technische und organisatorische Maßnahmen (TOMs)

- **Hintergrund:** Die TOMs sind die **konkreten Sicherheitsregeln** unserer Praxis. Sie beschreiben, *wie* wir die Daten technisch und organisatorisch schützen (z.B. durch Verschlüsselung oder Zugangskontrolle).
- **Ziel:** Sicherstellung der **Vertraulichkeit, Integrität und Verfügbarkeit** der Daten (**Art. 32 DSGVO**).
- **Praktisches Beispiel:** Die Anforderung der **Zugangskontrolle** in den TOMs erfüllen wir, indem jeder Mitarbeiter seinen eigenen Login und, für TI-Dienste, seinen **HBA (Heilberufsausweis)** nutzt.
- **Handout:** Muster siehe Anlage (Muster TOMs)

Datenschutzinformation an Betroffene/Patienten

- **Hintergrund:** Patienten haben ein Recht auf Transparenz. Sie müssen wissen, was mit ihren sensiblen Daten geschieht.
- **Inhalt:** Wir müssen in klarer Sprache informieren, *wer* die Daten *wofür* verarbeitet und *welche Rechte* der Patient hat (Auskunft, Löschung, Beschwerde).
- **Rechtsgrundlage: Art. 13 und 14 DSGVO**.

Handout: Muster siehe Anlage (Muster-Patienten-Datenschutzinformation)

2.3. Datenverarbeitung

Daten erfassen

- **Hintergrund:** Wann dürfen wir die Daten der Patienten überhaupt aufnehmen?
- **Rechtsgrundlage:** Die Erfassung ist durch den **Behandlungsvertrag** und die **gesetzliche Pflicht zur Dokumentation** gerechtfertigt (**§ 630f BGB**).
- **Erklärung:** Für die eigentliche Anamnese und Befunddokumentation benötigen Sie **keine separate, aktive Einwilligung** des Patienten; die gesetzliche Grundlage reicht aus.

Daten weitergeben (Brief, Telefon, verschlüsselte E-Mail, Signal, Patienten-Plattform)

- **Hintergrund:** Die Weitergabe von Gesundheitsdaten muss immer **sicher** erfolgen. Der Stand der Technik sind die Dienste der **Telematik-Infrastruktur (TI)**.
- **Brief:** Grundsätzlich zulässig, sofern der Empfänger sichergestellt ist (kein offener Umschlag).
- **Telefon:** Erlaubt, wenn die **Identität** des Gesprächspartners (z.B. anderer Arzt) **zweifelsfrei** geklärt ist.
- **Verschlüsselte E-Mail:** Zulässig, da die Vertraulichkeit gewahrt wird (**Art. 32 DSGVO**). Wird in der Praxis jedoch zunehmend durch **KIM (Kommunikation im Medizinwesen)** ersetzt, da dieser TI-Dienst Ende-zu-Ende verschlüsselt ist und als Standard gilt.
- **Patienten-Plattform (z.B. ePA):** Die sicherste Form der Bereitstellung. Der Arzt stellt Daten ein, aber der Patient **steuert** granular, wer wie lange darauf zugreifen darf (**Patientenhoheit**).
- **Signal/WhatsApp: Verboten!** Die fehlende Kontrolle über die Speicherung der Daten außerhalb der EU und die fehlenden Auftragsverarbeitungsverträge mit den Anbietern sind ein **Verstoß gegen Art. 44 ff. DSGVO** und **Art. 32 DSGVO**.

Daten Löschen (Aufbewahrungsfrist Ende, Löschverlangen des Patienten, Tod des Patienten)

- **Hintergrund:** Das **Recht auf Löschung** (**Art. 17 DSGVO**) ist nicht absolut.
- **Aufbewahrungsfrist Ende:** Wir müssen Patientenakten **mindestens 10 Jahre** nach Abschluss der **Behandlung** aufbewahren (**§ 630f BGB**). Die Pflicht zur Löschung besteht erst danach.
- **Löschverlangen des Patienten:** Dies können wir ablehnen, solange die **gesetzlichen Aufbewahrungspflichten** (**Art. 17 Abs. 3 lit. b DSGVO**) dem entgegenstehen.
- **Tod des Patienten:** Die Schweigepflicht und der Datenschutz bleiben bestehen. Die Daten werden nach Ablauf der 10-Jahres-Frist gelöscht.

Einwilligung (mündlich, kumulativ, schriftlich)

- **Hintergrund:** Die Einwilligung ist nur nötig, wenn keine andere gesetzliche Grundlage existiert (z.B. bei der **Weitergabe** von Daten an einen Betriebsarzt).
- **Mündlich:** Für einfache, unmittelbare Vorgänge (z.B. Terminanruf bei Angehörigen) ist dies ausreichend.
- **Schriftlich/Qualifiziert:** Bei hochsensiblen Daten oder Weitergaben an Dritte (Art. 9 Abs. 2 lit. a DSGVO). Die Einwilligung muss **freiwillig, informiert, spezifisch und widerrufbar** sein.
- **Kumulativ:** Achtung bei der Verknüpfung mehrerer Zwecke in einer Einwilligung.
- **Rechtsgrundlage: Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO**.

Handout: Muster siehe Anlage (Muster-Einwilligung)

2.4. Erfüllung der Patientenrechte

Wir sind verpflichtet, Anfragen von Patienten zu ihren Rechten **unverzüglich, spätestens innerhalb eines Monats**, zu beantworten.

Recht auf Auskunft

- **Rechtsgrundlage: Art. 15 DSGVO.**
- **Worum geht es?** Patienten können verlangen, Auskunft darüber zu erhalten, welche Daten wir verarbeiten, *woher* sie stammen und *an wen* sie weitergegeben werden.

Recht auf Löschung

- **Rechtsgrundlage: Art. 17 DSGVO.**
- **Erklärung:** Das Recht auf Löschung ist durch unsere 10-jährige Aufbewahrungspflicht in den meisten Fällen eingeschränkt.

Recht auf Daten-Übertragbarkeit

- **Rechtsgrundlage: Art. 20 DSGVO.**
- **Erklärung:** Dieses Recht ist auf unsere Praxis-Dokumentation meist nicht anwendbar. Es gilt nur für elektronische Daten, die der Patient selbst bereitgestellt hat und die aufgrund einer Einwilligung verarbeitet werden (z.B. ein übermittelter Blutdrucktagebuch-Datensatz).

Recht auf Sperrung/Einschränkung der Verarbeitung

- **Rechtsgrundlage: Art. 18 DSGVO.**
- **Erklärung:** Wenn ein Patient die Richtigkeit seiner Daten bestreitet, müssen wir die **Verarbeitung (z.B. die Weitergabe**) bis zur Klärung **einschränken** oder **sperren**.

---

3. ePA:

3.1. Fallstricke und Besonderheiten bei Kindern und Jugendlichen

Das Berechtigungsmanagement bei minderjährigen Patienten ist **deutlich komplexer** als bei Erwachsenen, da es vom Alter des Kindes und seiner **Einsichts- und Entscheidungsfähigkeit** abhängt.

Komplexes Berechtigungsmanagement

- **0 bis 15 Jahre:** Grundsätzlich üben die **Sorgeberechtigten** (Eltern) das Entscheidungsrecht über die ePA aus. Sie erhalten den Zugriff.
- **Ab 15 Jahren:** Der Jugendliche wird **selbst handlungsfähig** in Bezug auf die ePA. Er **allein** entscheidet, ob er eine ePA haben möchte und wer darauf zugreifen darf.
    - **Hintergrund:** Der Gesetzgeber folgt hier dem Grundsatz der ausreichenden Einsichtsfähigkeit.
    - **Rechtsgrundlage:** Analoge Anwendung von **§ 362 SGB V** (Zugangsberechtigung). Die Sorgeberechtigten **verlieren automatisch das Zugriffsrecht** auf die ePA, sobald der Patient 15 Jahre alt wird – es sei denn, der Jugendliche erteilt ihnen eine Vollmacht.

Wahrung der therapeutischen Beziehung

- **Hintergrund:** Bei psychologischen oder psychiatrischen Behandlungen von Jugendlichen kann die Offenlegung der Daten (z.B. den Sorgeberechtigten) die therapeutische Beziehung gefährden.
- **Ihre Pflicht:** Bei der Einstellung von Dokumenten in die ePA (z.B. psychotherapeutische Befunde) besteht für Sie eine **besondere Informationspflicht**. Sie müssen den Patienten (oder den Jugendlichen ab 15 Jahren) **aktiv auf sein Widerspruchsrecht hinweisen**.
- **Konsequenz:** Widerspricht der Patient der Einstellung eines sensiblen Dokuments, müssen Sie dies akzeptieren, und das Dokument darf **nicht** in die ePA.

3.2. Datenschutzrechtliche Problematik: Feingranulare Einsicht

Die datenschutzrechtliche Problematik betrifft alle sensiblen Patienten-Daten (z.B. aus der Psychiatrie/Psychologie), die **nicht** für alle zugreifenden Ärzte sichtbar sein sollen.

Das Problem der Standard-Freigabe: Erteilt der Patient einem Arzt (z.B. dem Hausarzt) Zugriff auf die ePA, hat dieser standardmäßig Zugriff auf **alle** nicht verborgenen Dokumente – also potenziell auch auf die sensiblen Berichte des Psychiaters.

Die mangelnde Granularität (Design-Lücke): Die ePA bietet dem Patienten **keine einfache, vorgelagerte Möglichkeit**, eine allgemeine Regel einzustellen, wie: *"Alle Dokumente aus der Kategorie 'Psychiatrie' für alle Fachbereiche verbergen, außer für den Psychiater selbst."*

- **Konsequenz:** Der Patient muss **jede einzelne Eingabe** des Psychiaters/Psychologen über seine ePA-App **nachträglich manuell verbergen** ("verschatten"), damit andere Ärzte sie nicht sehen können. Dies ist umständlich und fehleranfällig.

Stigmatisierung und Diskriminierung

- **Hintergrund:** Die zentrale Speicherung von sensiblen Diagnosen (z.B. psychische Erkrankungen, HIV) in der ePA erhöht das Risiko, dass Patienten bei späteren Entscheidungen (z.B. Abschluss einer Versicherung) benachteiligt werden.
- **Patienten-Kontrolle ist Pflicht:** Wir müssen die Patienten aktiv auf ihre **Rechte zur Kontrolle** hinweisen:
    1. **Dokumente Verbergen:** Patienten können jedes sensible Dokument über ihre App **für alle anderen Ärzte unsichtbar** machen.
    2. **Abrechnungsdaten:** Patienten müssen den Abrechnungsdaten (die Diagnosen enthalten) aktiv **widersprechen oder sie verbergen**, da diese sonst ebenfalls für jeden zugreifenden Arzt sichtbar sind.

Handout: Muster siehe Anlage (Muster- Widerspruch gegen die Abrechnungsdaten in der ePA)

3.3. Bedenken gegenüber der EU-Erweiterung der ePA (EHDS)

Der Blick geht über Deutschland hinaus: Die Europäische Union plant die Einführung des **European Health Data Space (EHDS)**, eines europäischen Gesundheitsdatenraums.

- **1. Primärnutzung (Behandlungsvorteil):** Patienten sollen ihre Daten **grenzüberschreitend** mitführen und Ärzte in anderen EU-Ländern sollen darauf zugreifen können (z.B. Medikationsplan).
- **2. Sekundärnutzung (Forschung/Planung – Die Bedenken):** Pseudonymisierte Daten aus der ePA sollen für Forschungszwecke, Gesundheitsplanung und Innovation bereitgestellt werden.

Zeitplan und das Opt-out-Prinzip

- **Geplanter Zeitplan:** Die ersten nationalen Datenaustauschstellen sollen voraussichtlich **ab 2026/2027** ihre Arbeit aufnehmen. Die vollständige Umsetzung des EHDS wird Jahre dauern.
- **Datenschutzrechtliche Herausforderung:** Die sekundäre Nutzung der Daten soll weitgehend nach dem **Opt-out-Prinzip** erfolgen. Das bedeutet:
  - Wenn Patienten der Nutzung ihrer Daten für Forschungszwecke **nicht aktiv widersprechen**, werden ihre pseudonymisierten Daten verwendet.
- **Ihre Pflicht:** Wir müssen die Patienten über dieses **Widerspruchsrecht** gegenüber der Sekundärnutzung ihrer Daten **informieren**.

Fazit ePA: Die ePA ist ein Fortschritt, aber sie erfordert eine **höhere Wachsamkeit und Aufklärungspflicht** seitens des Arztes. Wir müssen unseren Patienten die Kontrollwerkzeuge (Widerspruch, manuelles Verbergen) aktiv an die Hand geben. Nur so können wir die Patientenhoheit über sensible Daten wirklich gewährleisten.

---

4. Typische Fehler auf Praxis-Webseiten

Die Website ist unser digitales Aushängeschild, aber sie ist auch eine **öffentliche Fläche**, die von Aufsichtsbehörden und Abmahnern routinemäßig geprüft wird. Fehler hier sind **sichtbar, leicht feststellbar und werden teils empfindlich sanktioniert.** Wir sprechen heute über die typischen Fehler und die rechtlichen Konsequenzen.

4.1. Unvollständige Datenschutzerklärung

Der häufigste und gefährlichste Fehler ist eine **unvollständige oder fehlerhafte Datenschutzerklärung (DSE)**. Viele verwenden veraltete oder unvollständige Generatoren.

- **Der Kernfehler: Die fehlende Zweiteilung**
  - Das Problem ist, dass Webseitenprogrammierer oft **Generatoren** verwenden oder Texte kopieren, die **nur die Datenverarbeitung der Website** (Server-Logs, Cookies, Google Maps) abdecken.
  - **Was fehlt:** Diese extern generierten Texte ignorieren meist die **individuelle Datenverarbeitung im Kerngeschäft der Arztpraxis**, nämlich die Verarbeitung von **Gesundheitsdaten** im Behandlungsfall.
  - **Die Notwendigkeit der Zweiteilung:** Unsere DSE muss daher klar in **zwei Bereiche** unterteilt sein:
    1. **Webseiten-Datenverarbeitung:** Was passiert, wenn ein Nutzer die Seite besucht (**Art. 6 Abs. 1 lit. f DSGVO**).
    2. **Praxis-Datenverarbeitung (Kerngeschäft):** Die Verarbeitung von sensiblen Gesundheitsdaten im Behandlungsfall (**Art. 9 Abs. 2 lit. h DSGVO**).

- **Fehlende Kerndatenverarbeitung (Der größte Verstoß):** Wenn der Teil zur Verarbeitung von Gesundheitsdaten fehlt, verletzen wir die Informationspflicht an der wichtigsten Stelle. Wir klären den Patienten **nicht** darüber auf, welche Diagnosen, Befunde und Abrechnungsdaten wir zu welchem Zweck verarbeiten.
  - **Rechtsgrundlage: Art. 13 DSGVO** (Informationspflicht) i.V.m. **Art. 9 DSGVO** (sensible Daten).
  - **Repressalie:** Bei einer schwerwiegenden Verletzung der Informationspflicht drohen **Bußgelder** durch die Aufsichtsbehörden. Diese Fehler sind leicht feststellbar und damit ein attraktives Angriffsziel für Prüfungen.
- **Cookie-Banner und Werbetracker:** Die reine DSE reicht nicht. Wenn wir Tracking-Tools nutzen (z.B. Google Analytics) oder Cookies setzen, müssen wir vorab die **aktive Einwilligung** der Nutzer einholen.
  - **Rechtsgrundlage: § 25 TTDSG** (Teleschutzdatenschutzgesetz) verlangt die aktive, informierte Einwilligung (Opt-in-Lösung) für alle nicht technisch notwendigen Cookies.
  - **Konsequenz:** Ein fehlendes oder falsch konfiguriertes Cookie-Banner (z.B. nur ein "OK"-Button ohne Ablehnungsmöglichkeit) wird als **illegales Auslesen von Endgeräten** betrachtet.
- **Formfehler:** Oft wird der **Name des Datenschutzbeauftragten** (falls vorhanden) nicht genannt oder der Praxis-Inhaber führt sich selbst als Datenschutzbeauftragter auf, obwohl er der „Verantwortliche“ ist und damit nach Art37 DSGVO einen Interessenkonflikt-Verstoß provoziert.
- das **Beschwerderecht bei der Aufsichtsbehörde** vergessen. Auch dies sind formelle, aber ahndbare Mängel.

Viele Praxen binden Dienste Dritter ein, ohne die rechtlichen Konsequenzen zu beachten.

Google Maps und Google Fonts

- **Das Problem:** Wird Google Maps oder Google Fonts (nicht lokal) in die Website eingebunden, wird die **IP-Adresse des Nutzers** an Google in die **USA** übertragen, sobald der Nutzer die Seite lädt.
- **Rechtsgrundlage:** Hier liegt ein sogenannter **Drittlandtransfer** vor. Da die USA **kein** sicheres Drittland nach DSGVO ist, ist dieser Transfer nur mit **expliziter Einwilligung** und **zusätzlichen Garantien** zulässig (**Art. 44 ff. DSGVO**).
- **Repressalie:** In der Vergangenheit wurden Praxen und Website-Betreiber bereits wegen der unzulässigen Übermittlung von IP-Adressen an Google **abgemahnt und verklagt** (z.B. durch Urteile der Landgerichte). Sie handeln hier ohne rechtliche Grundlage.

Doctolib & andere Buchungsportale

- **Das Problem:** Wenn das Doctolib- oder ein ähnliches Dienstleistungs-Widget **direkt in die Praxis-Website eingebettet** ist, beginnt bereits dort die Datenverarbeitung durch Doctolib.
- **Ihre Pflicht:** Sie müssen in Ihrer Datenschutzerklärung auf diese **gemeinsame Verantwortlichkeit** hinweisen und den **Vertrag zur gemeinsamen Verantwortlichkeit (Joint Controllership Agreement)**, den Sie mit dem Anbieter schließen müssen, erwähnen.
  - **Rechtsgrundlage: Art. 26 DSGVO (Gemeinsame Verantwortlichkeit).**
  - **Konsequenz: Fehlt der Hinweis in der DSE oder der Vertrag, begehen Sie einen schwerwiegenden Dokumentationsfehler**.

Handout: Muster siehe Anlage (Muster-Datenschutzerklärung für Websites)

4.2. Unvollständiges Impressum

Das Impressum ist keine Datenschutzvorschrift, aber es ist eine **gesetzliche Pflicht** (Telemediengesetz), deren Fehlen sofort zur **Abmahnung** führt – oft die Initialzündung für weitere Datenschutzprüfungen.

- **Fehlende Pflichtangaben:** Das Impressum muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Es muss zwingend enthalten:
  - Name und Anschrift des Arztes/der Praxis.

    - Kontaktinformationen (E-Mail und Telefonnummer!).
    - Die zuständige **Kammer** (z.B. Ärztekammer Nordrhein).
    - Die **gesetzliche Berufsbezeichnung** (z.B. "Arzt") und der Staat, in dem sie verliehen wurde (Deutschland).
    - Berufsrechtliche Regelungen (z.B. Berufsordnung).
- **Rechtsgrundlage: § 5 TMG** (Telemediengesetz) und **§ 55 RStV** (Rundfunkstaatsvertrag).
- **Repressalie:** Das Fehlen dieser Angaben stellt einen **Wettbewerbsverstoß** dar und kann direkt zu **kostenpflichtigen Abmahnungen** durch Wettbewerber oder spezialisierte Kanzleien führen.

Handout: Muster siehe Anlage (Muster-Impressum)

Wir kommen zum Abschluss unseres heutigen Vortrags, und dieser Punkt ist besonders wichtig, da er zeigt, dass der Datenschutz keine theoretische Bürokratie ist, sondern **aktive Gerichtsverfahren und Bußgelder** nach sich zieht. Wir sprechen über aktuelle Urteile, die als **Warnsignale** dienen müssen.

---

5. Aktuelle Urteile

Webseite (Google Fonts)

- **Der Fall:** Ein Gericht entschied über einen Fall, bei dem eine Website die **Google Fonts** nicht lokal gespeichert hatte, sondern von Google-Servern in den USA nachlud. Dabei wurde die **IP-Adresse** des Nutzers an Google übermittelt.
- **Urteil und Bedeutung:** Das Gericht sah in der unaufgeforderten Weitergabe der IP-Adresse an Google in die USA ohne Einwilligung des Nutzers einen **unzulässigen Drittlandtransfer** und eine **Verletzung des allgemeinen Persönlichkeitsrechts**. Der Website-Betreiber wurde zu **Schadensersatz** verurteilt.
- **Ihre Konsequenz:** Dies belegt, dass selbst die kleinste technische Einbindung von US-Diensten ohne vorherige, aktive Einwilligung (Opt-in) des Nutzers ein **rechtliches Risiko** darstellt. Dies gilt für Google Maps, Google Fonts und ähnliche Dienste. Sie müssen diese Dienste entweder **lokal speichern** oder nur **mit aktiver Zustimmung** einbinden.
- **Rechtsgrundlage: Art. 44 ff. DSGVO** (Drittlandtransfer).

Nutzung von Messenger Diensten (z.B. WhatsApp)

- **Der Fall:** Verschiedene Aufsichtsbehörden haben in den letzten Jahren Bußgelder gegen Ärzte und Kliniken verhängt, die Patientendaten (Bilder, Befunde, Absprachen) über **WhatsApp** oder ähnliche, nicht-DSGVO-konforme Messenger ausgetauscht haben.
- **Urteil und Bedeutung:** Die Behörden stellten fest, dass die Messenger-Dienste die Daten oft auf Servern in den USA speichern und die notwendige **Ende-zu-Ende-Verschlüsselung** sowie die **Auftragsverarbeitungsverträge (AVV)** nach europäischen Standards fehlen. Die Nutzung stellt einen **groben Verstoß gegen die Datensicherheit** dar.
- **Ihre Konsequenz:** Die Nutzung von WhatsApp oder ähnlichen Messengern zur Kommunikation mit Patienten über Behandlungsinhalte ist **strikt untersagt**. Das Risiko ist ein **Bußgeld** wegen Verletzung der **Art. 32 und Art. 44 ff. DSGVO**. Nutzen Sie stattdessen die gesicherten Kanäle der TI, wie **KIM**.

Video-Sprechstunde

- **Der Fall:** Während der Pandemie gerieten viele Anbieter von Videosprechstunden in den Fokus. Die Aufsichtsbehörden prüften, ob die Anbieter die **technischen und organisatorischen Anforderungen (TOMs)** der DSGVO und der Kassenärztlichen Vereinigung (KBV) erfüllten.

- **Urteil und Bedeutung:** Praxen, die unzertifizierte Anbieter nutzten, die beispielsweise keine ausreichende **Verschlüsselung** oder keinen korrekten **Auftragsverarbeitungsvertrag** (**Art. 28 DSGVO**) vorlegen konnten, wurden zur Kündigung des Vertrages aufgefordert und mussten mit Sanktionen rechnen.
- **Ihre Konsequenz:** Sie dürfen nur Videosprechstunden-Anbieter nutzen, die **speziell für den Gesundheitsbereich zertifiziert** sind (z.B. durch die KBV) und die Ihnen einen **korrekten Auftragsverarbeitungsvertrag (AVV)** vorlegen können. Ohne AVV begehen Sie einen **formellen Dokumentationsfehler**, der mit Bußgeldern belegt werden kann (**Art. 83 Abs. 4 DSGVO**).

Schlusswort

Diese Urteile zeigen: Datenschutz ist gelebte Praxis. Die Fehler sind oft klein (ein falscher Link, eine bequeme App), aber die Repressalien können groß sein. Nutzen Sie die Musterdokumente und die sicheren Kanäle der TI – das ist der beste Schutz für Ihre Patienten und Ihre Praxis.

Zusammenfassung und Handlungsbedarf

Lassen Sie uns den größten Fehler vermeiden: Die Einhaltung der Gesetze ist der **günstigste Schutz**.

1. **Aktualisieren Sie Ihre DSE:** Stellen Sie die **Zweiteilung** sicher: **Website** und **Kerngeschäft Praxis-Daten**.
2. **Prüfen Sie Ihr Cookie-Banner:** Es muss eine **Opt-in-Lösung** sein (Ablehnung muss genauso einfach sein wie die Zustimmung).
3. **Vervollständigen Sie Ihr Impressum:** Geben Sie alle geforderten Kontakt- und Kammerdaten an.

Wenn wir diese einfachen Hausaufgaben erledigen, reduzieren wir das Risiko von teuren Abmahnungen und Bußgeldern auf ein Minimum.