



KLEIN.

NOTFALLPLAN

PRAXIS- DURCHSUCHUNG

Checkliste für Ärzte, Zahnärzte, MVZ und Praxisteams

DIE ERSTEN 30 MINUTEN ENTSCHEIDEN

- ☐ Ruhe bewahren und keine Angaben zur Sache machen.
- ☐ Durchsuchungsbeschluss verlangen und Verteidiger sofort anrufen.
- ☐ Nichts freiwillig herausgeben oder ungeprüft unterschreiben.
- ☐ Maßnahme begleiten, dokumentieren und Praxisbetrieb sichern.

SOFORTHILFE

0721 1510 1010

Matthias Klein

Fachanwalt für Strafrecht und Medizinrecht

Strafverteidigung für Ärzte. Medizinrecht inklusive.

Ausdrucken, Zuständigkeiten eintragen und am Empfang sowie in der Notfallmappe bereithalten.

Vor dem Ernstfall · Notfallvorsorge

Dieser Plan verbindet strafprozessuale Sofortmaßnahmen mit medizinrechtlichem Datenschutz und einem belastbaren Wiederanlaufkonzept.

WICHTIGER GRUNDSATZ

Eine Durchsuchung darf nicht körperlich behindert werden. Es werden aber keine Angaben zur Sache gemacht, keine freiwilligen Einwilligungen erteilt und Einwände sachlich dokumentiert.

Vorbereitung - einmal jährlich aktualisieren

- ☐ Durchsuchungskoordinator, Stellvertretung, IT-Verantwortlichen und Patientenkoordinator namentlich festlegen.
- ☐ Aktuelle Notfallkontakte offline hinterlegen: Verteidiger, IT-Dienstleister, Softwarehaus, Datenschutzbeauftragter, Telefonieanbieter und Versicherer.
- ☐ Verzeichnis aller Praxisstandorte, Server, Sicherungsmedien, Cloud-Dienste, Mobiltelefone, Fahrzeuge und häuslichen Arbeitsplätze erstellen.
- ☐ Wiederherstellung aus dem Backup praktisch testen und Ergebnis dokumentieren.
- ☐ Ersatzgeräte, Notfalltelefon, Papierformulare und einen getrennt verwahrten Notfall-Datenträger bereithalten.

Ihre vorbereiteten Kontaktdaten

Durchsuchungskoordinator	
Stellvertretung	
IT-Dienstleister / Notruf	
Praxissoftware-Support	
Datenschutzbeauftragter	
Telefonie / Rufumleitung	

1. Die ersten 30 Minuten

Ruhe bewahren. Schweigen. Nichts freiwillig herausgeben. Sofort den Verteidiger anrufen.

0-5 Minuten · Empfang und Erstkontakt

- ☐ Praxisleitung und Durchsuchungskordinator sofort informieren.
- ☐ Matthias Klein anrufen: 0721 1510 1010.
- ☐ Dienstausweise zeigen lassen; Namen, Behörde und Erreichbarkeit der Einsatzleitung notieren.
- ☐ Durchsuchungsbeschluss und Anlagen vollständig aushändigen lassen oder fotografieren.
- ☐ Aktenzeichen, Tatvorwurf, betroffene Personen, Räume, Fahrzeuge, Zeitraum und gesuchte Gegenstände notieren.
- ☐ Sachlich mitteilen: „Wir behindern rechtmäßige Maßnahmen nicht. Wir machen keine Angaben zur Sache und stimmen freiwilligen Sicherstellungen nicht zu.“

5-15 Minuten · Umfang und Sphären klären

- ☐ Klären, gegen wen sich die Maßnahme richtet: Arzt, Mitarbeiter, Praxisgesellschaft/MVZ oder Dritte.
- ☐ Nur die im Beschluss bezeichneten Praxisräume, privaten Wohnräume, Nebenräume, Garagen und Fahrzeuge zuordnen.
- ☐ Private Räume, Zimmer von Familienangehörigen, Untermietflächen und Räume anderer Berufsträger ausdrücklich kennzeichnen.
- ☐ Jeden Ermittlungsbeamten möglichst durch eine eingewiesene Person begleiten lassen.
- ☐ Keine Unterlagen vernichten, verändern, verstecken, nachträglich ergänzen oder elektronisch löschen.
- ☐ Patientenbetrieb diskret organisieren; Notfälle und medizinisch unaufschiebbare Behandlungen sicherstellen.

15-30 Minuten · Sicherstellung dokumentieren

- ☐ Bei jeder Übergabe klarstellen: keine freiwillige Herausgabe; förmliche Sicherstellung/Beschlagnahme dokumentieren.
- ☐ Der Sicherstellung und Durchsicht vorsorglich widersprechen und den Widerspruch protokollieren lassen.
- ☐ Bei Patientenakten und Massendaten auf Daten unbeteiligter Patienten, Zweckbindung und sachgerechte Filterung hinweisen.
- ☐ Geräte, SIM-Karten, Datenträger, Seriennummern, Konten, Verzeichnisse, Zeiträume und Datenkopien einzeln erfassen.
- ☐ Durchsuchungsbescheinigung, Beschluss, Anlagen und vollständiges Sicherstellungs-/Beschlagnahmeverzeichnis verlangen.

NICHT UNTERSCHREIBEN

Keine unklaren Erklärungen, Einwilligungen oder „freiwilligen Herausgaben“ ungeprüft unterzeichnen. Ein Widerspruch stoppt die Maßnahme regelmäßig nicht, dokumentiert aber die fehlende Freiwilligkeit.

2. Rollenplan für das Praxisteam

Jeder kennt seine Aufgabe – niemand äußert sich spontan zum Sachverhalt.

Rolle	Aufgabe im Ernstfall	Name / Vertretung
Empfang	Beamte in einen geeigneten Raum führen; Praxisleitung informieren; keine Sachauskünfte.	
Koordination	Beschluss sichern; Verteidiger anrufen; Begleitpersonen einteilen; Einwände bündeln.	
IT	Systemlandschaft sachlich benennen; keine Löschungen; Ausfallfolgen und Ersatzlösungen dokumentieren.	
Patientenbetrieb	Diskrete Umleitung; Notfälle versorgen; Terminbetrieb stabilisieren.	
Dokumentation	Zeiten, Personen, Räume, Maßnahmen, Äußerungen, Daten und Gegenstände protokollieren.	
Privatbereich/Fahrzeuge	Familien- und Drittsphären kennzeichnen; private Geräte und Fahrzeuge zuordnen.	
Kommunikation	Anfragen von Patienten, Presse, KV/KZV, Kassen und Kammer bündeln.	

Was Mitarbeiter sagen dürfen

EMPFOHLENE FORMULIERUNG

„Ich mache keine Angaben zum Sachverhalt. Bitte wenden Sie sich an die Praxisleitung und unseren Rechtsanwalt. Bei rein organisatorischen Fragen helfe ich Ihnen gern.“

Was niemand spontan erklären sollte

- ☐ Warum eine Leistung abgerechnet, delegiert, dokumentiert oder freigegeben wurde.
- ☐ Wer auf Abrechnung, Praxissoftware, Signaturmittel, Patientenakten oder Konten Zugriff hatte.
- ☐ Ob etwas „immer so gemacht“, „nur ein Versehen“ oder „ohnehin üblich“ gewesen sei.
- ☐ Welche Patienten, Abrechnungsfälle, Geräte oder privaten Nachrichten auffällig sein könnten.
- ☐ Passwörter, PINs oder Entsperrcodes ohne konkrete anwaltliche Rücksprache.

KEINE INTERNEN ERMITTLUNGEN

Keine Rundmails, Chats, Telefonketten oder abgestimmten Erinnerungen. Keine nachträglichen Dokumentationseinträge.

3. Patientendaten und Berufsgeheimnisse

Arztpraxen enthalten regelmäßig Gesundheitsdaten zahlreicher unbeteiligter Patienten.

Patientenakten, Datenbanken und Mischbestände

- ☐ Auf ärztliche Schweigepflicht und Daten unbeteiligter Patienten ausdrücklich hinweisen.
- ☐ Bezug zum Beschluss prüfen: Person, Zeitraum, Behandlungsfall, Abrechnungsziffer und Datenkategorie.
- ☐ Bei Mischakten oder Datenbanken sachgerechte Sichtung, Suchbegriffe, zeitliche Filterung und Trennung anregen.
- ☐ Notieren, welche fremden Patientendaten eingesehen, kopiert, exportiert oder mitgenommen werden.
- ☐ Keine Schweigepflichtentbindungen selbst einholen und Patienten während der Maßnahme nicht zum Sachverhalt kontaktieren.
- ☐ Behandlungsnotwendige Datenverfügbarkeit sichern: Medikation, Allergien, Notfallbefunde und Terminlisten müssen für die Versorgung erreichbar bleiben.

Verteidigungsunterlagen und getrennte Sphären

- ☐ Verteidigerkorrespondenz und Verteidigungsunterlagen sofort eindeutig kennzeichnen.
- ☐ Unterlagen anderer Ärzte, Therapeuten, Gesellschaften oder Familienangehöriger klar zuordnen.
- ☐ Private Unterlagen und Daten anderer Haushaltsmitglieder räumlich und technisch kenntlich machen.
- ☐ Bei der Praxis eines Nichtbeschuldigten auf konkrete Zweck- und Gegenstandsbindung hinweisen.

RECHTLICHER KERN

Der besondere Schutz von Berufsgeheimnisträgern verlangt bei der Durchsuchung einer Arztpraxis besonders sorgfältige Beachtung von Tatverdacht und Verhältnismäßigkeit. Der Beschlagnahmeschutz ist nicht pauschal; Verfahrensrolle, Gewahrsam und Tatbezug sind im Einzelfall entscheidend.

Verhältnismäßigkeit konkret dokumentieren

- ☐ Welche Bereiche, Personen oder Daten haben erkennbar keinen Bezug zum Tatvorwurf?
- ☐ Welche mildere Maßnahme wäre möglich: gezielte Herausgabe, gefilterter Export, forensische Kopie oder Versiegelung?
- ☐ Welche Nachteile entstehen für Patientenversorgung, Datenschutz und Praxisbetrieb?
- ☐ Wie lange waren Räume, Systeme, Telefone oder Fahrzeuge nicht nutzbar?
- ☐ Wurden Daten unbeteiligter Patienten oder Dritter in erheblichem Umfang erfasst?

4. Wohnräume, Fahrzeuge und persönliche Geräte

Durchsuchungen können parallel Praxis, Wohnung, Nebenräume, Fahrzeuge und private Mobilgeräte erfassen.

Bei einer Durchsuchung der Wohnung

- ☐ Beschluss auf Anschrift, betroffene Person, Nebenräume, Keller, Garage und weitere Wohneinheiten prüfen.
- ☐ Zimmer, Schränke und Geräte von Ehepartnern, Kindern, Mitbewohnern oder Gästen ausdrücklich als Drittsphäre kennzeichnen.
- ☐ Private und berufliche Unterlagen nicht spontan erklären oder selbst durchsuchen; Zuordnung nur sachlich benennen.
- ☐ Keine privaten Nachrichten löschen, Geräte zurücksetzen, Cloud-Konten abmelden oder Fernlösungen auslösen.
- ☐ Mitgenommene Ausweise, Schlüssel, Karten, Medikamente und medizinische Hilfsmittel sofort dokumentieren.

Bei Fahrzeugen

- ☐ Kennzeichen, Halter, regelmäßige Nutzer und Fahrzeugstandort notieren.
- ☐ Geschäftliche und private Fahrzeuge sowie Fahrzeuge Dritter klar zuordnen.
- ☐ Fahrzeugschlüssel, Fahrzeugschein, Tank-/Ladekarten, Parkkarten und mobile Datenträger einzeln dokumentieren.
- ☐ Bei betriebsnotwendigen Praxisfahrzeugen konkrete Ausfallfolgen benennen und Herausgabe bzw. Kopie notwendiger Unterlagen anregen.

Persönliche Daten vorsorglich sichern

- ☐ Verschlüsseltes Backup wichtiger privater Dokumente getrennt vom Wohn- und Praxisstandort aufbewahren.
- ☐ Wiederherstellungscodes für E-Mail, Apple-/Google-/Microsoft-Konten und Passwortmanager sicher offline hinterlegen.
- ☐ Notfallliste mit Ausweisnummern, Banken, Versicherungen, Familienkontakten und Medikamenten führen.
- ☐ Private Fotos, Kontakte und Kalender regelmäßig sichern; Wiederherstellung auf einem Ersatzgerät testen.
- ☐ Berufliche Patientendaten nicht unkontrolliert in privaten Clouds, Foto-Apps, Messengern oder privaten Backups spiegeln.
- ☐ Backup-Medien verschlüsseln, Zugriff beschränken und Aufbewahrungsort dokumentieren.

KEIN VERHALTEN IM LAUFENDEN ZUGRIFF

Die Vorsorge erfolgt vor dem Ernstfall. Während der Durchsuchung dürfen keine Daten gelöscht, verschoben, versteckt oder aus der Ferne unzugänglich gemacht werden.

5. Praxisbetrieb nach Mitnahme von IT und Mobiltelefonen

Rechtmäßiger, datenschutzgerechter Wiederanlauf – ohne Beweismittel zu verändern.

Technische Vorsorge

- ☐ 3-2-1-Prinzip umsetzen: drei Datenkopien, auf zwei unterschiedlichen Medien, davon eine verschlüsselte Kopie räumlich getrennt.
- ☐ Automatisierte Backups der Praxissoftware, Dokumente, Telefonkonfiguration und Servereinstellungen einrichten.
- ☐ Mindestens eine Sicherung logisch oder physisch vom Produktivsystem trennen.
- ☐ Wiederherstellung regelmäßig praktisch testen – nicht nur Backup-Protokolle kontrollieren.
- ☐ Notfall-Laptop und vorkonfigurierte Ersatztelefone ohne Patientendaten bereithalten.
- ☐ Rufumleitung und Ersatzrufnummer schriftlich festlegen; Zugangsdaten sicher und getrennt verfügbar halten.
- ☐ Papier-Notbetrieb vorbereiten: Aufnahme, Einwilligung, Rezept-/Verordnungsworkflow, Befundnotizen, Termin- und Rückruflisten.
- ☐ Kontaktdaten von Laboren, Apotheken, Kliniken, IT, Softwarehaus, KV/KZV und Datenschutzbeauftragtem offline vorhalten.

Unmittelbar nach der Mitnahme

- ☐ Mit dem Verteidiger klären, welche Geräte und Daten betroffen sind und welche Herausgabe-, Kopier- oder Spiegelungsanträge gestellt werden.
- ☐ IT-Dienstleister aktivieren; keine eigenmächtigen Änderungen an verbleibenden Systemen mit Beweisbezug vornehmen.
- ☐ Rufnummern und dienstliche Kommunikation auf Ersatzgeräten wiederherstellen; private Messenger nicht als ungeprüften Ersatz nutzen.
- ☐ Patienten neutral über organisatorische Einschränkungen informieren; keine Angaben zum Verfahren.
- ☐ Notbetrieb dokumentieren: Beginn, ausgefallene Systeme, Ersatzprozesse, Verantwortliche und Rückkehr in den Regelbetrieb.
- ☐ Papiernotizen später vollständig und mit tatsächlichem Erstellungs- und Übertragungsdatum in die Patientenakte übernehmen.
- ☐ Datenschutz- oder sonstige Meldepflichten prüfen lassen; keine vorschnelle Eigenmeldung.

Kritische Funktionen und Ersatzlösung

Kritische Funktion	Vorbereitete Ersatzlösung	Verantwortlich / Kontakt
Telefon / Rufumleitung		
Terminkalender		
Patientenstammdaten		
Medikation / Notfälle		

Kritische Funktion	Vorbereitete Ersatzlösung	Verantwortlich / Kontakt
Labor / Befundabruf		
Abrechnung / Kasse		
E-Mail / sichere Kommunikation		
Praxissoftware / Server		

6. Übergabeblatt für Ermittlungsbeamte

Zu Beginn übergeben. Es ersetzt keine Einzelfallberatung und hindert rechtmäßige Maßnahmen nicht.

ERKLÄRUNG ZUR DURCHSUCHUNG

Die Praxis wird rechtmäßige Maßnahmen nicht behindern.

Es werden keine Angaben zur Sache gemacht. Fragen zum Tatvorwurf, zu Abrechnungen, Behandlungen, Dokumentation, Delegation, Zuständigkeiten oder internen Abläufen werden erst nach anwaltlicher Beratung beantwortet.

Eine freiwillige Einwilligung in Durchsuchung, Durchsicht, Sicherstellung oder Herausgabe wird nicht erteilt. Wir bitten um förmliche Dokumentation und Aufnahme unseres Widerspruchs.

Bitte beachten Sie die ärztliche Schweigepflicht, die Gesundheitsdaten unbeteiligter Patienten und getrennte private oder fremde Sphären. Bitte begrenzen Sie die Maßnahme auf die im Beschluss bezeichneten Personen, Räume, Fahrzeuge, Zeiträume, Sachverhalte und Gegenstände.

Bitte ermöglichen Sie die telefonische Kontaktaufnahme mit unserem Rechtsanwalt und erstellen Sie ein vollständiges, individualisiertes Verzeichnis aller sichergestellten oder beschlagnahmten Gegenstände und Daten.

Verteidiger: Matthias Klein · Fachanwalt für Strafrecht und Medizinrecht
Telefon: 0721 1510 1010

Ort / Datum	Praxis / Standort
Name / Funktion	Unterschrift
Entgegengenommen durch	Uhrzeit
Bemerkung	

HINWEIS FÜR DEN EMPFANG

Ruhig aushändigen. Wird die Entgegennahme abgelehnt, Uhrzeit, Name und Ablehnung im internen Protokoll notieren.

7. Durchsuchungsprotokoll

Zeitnah und sachlich dokumentieren. Keine Bewertungen, Spekulationen oder Schuldeingeständnisse.

Datum / Beginn / Ende	
Behörde / Dienststelle	
Aktenzeichen	
Einsatzleitung / Telefon	
Beschuldigter / Betroffener	
Tatvorwurf laut Beschluss	
Durchsuchte Standorte / Fahrzeuge	
Anwesender Staatsanwalt	
Verteidiger kontaktiert / Uhrzeit	

Verlauf und besondere Vorkommnisse

Uhrzeit	Raum / Maßnahme / Äußerung / Einwand	Beamter / Begleitperson

Uhrzeit	Raum / Maßnahme / Äußerung / Einwand	Beamter / Begleitperson

7a. Fortsetzung Durchsuchungsprotokoll

Zusätzlicher Raum für handschriftliche Einträge.

Uhrzeit	Raum / Maßnahme / Äußerung / Einwand	Beamter / Begleitperson

8. Sicherstellungs-, Daten- und IT-Verzeichnis

Jeder Gegenstand und jeder Datenexport muss später eindeutig zugeordnet werden können.

Nr.	Gegenstand / Datei / Datenbestand	Zeitraum / Bezug	Seriennr. / Speicherort	Kopie / Filter / Umfang	Widerspruch
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐
9					☐

Vor Abschluss der Maßnahme

- ☐ Bereiche außerhalb des Beschlusses dokumentiert.
- ☐ Gegenstände individualisiert; keine bloßen Sammelbezeichnungen.
- ☐ Datenkopien nach Quelle, Suchbegriffen, Filter, Zeitraum und Umfang beschrieben.
- ☐ Widerspruch und fehlende freiwillige Herausgabe vermerkt.
- ☐ Betriebsnotwendige Rückgaben, Kopien oder Fristen angesprochen.
- ☐ Kopien aller Dokumente erhalten.

8a. Fortsetzung Sicherstellungsverzeichnis

Zusätzlicher Raum für Geräte, Datenträger, Mobiltelefone, Unterlagen und Datenkopien.

Nr.	Gegenstand / Datei / Datenbestand	Zeitraum / Bezug	Seriennr. / Speicherort	Kopie / Filter / Umfang	Widerspruch
10					☐
11					☐
12					☐
13					☐
14					☐
15					☐
16					☐
17					☐
18					☐
19					☐
20					☐

Sofort notwendige Ersatzbeschaffung / Freigabe

Betroffenes System / Gerät	Konkrete Ausfallfolge	Ersatz / Antrag / Frist
----------------------------	-----------------------	-------------------------

9. Nach der Durchsuchung

Strafverfahren, Datenschutz, Praxisbetrieb und medizinrechtliche Folgerisiken gemeinsam steuern.

Noch am selben Tag

- ☐ Team anweisen: keine externen oder internen Sachverhaltsdiskussionen.
- ☐ Beschluss, Fotos, Protokolle, Notizen und Verzeichnisse zentral und unverändert sichern.
- ☐ Begleitpersonen getrennte Gedächtnisprotokolle erstellen lassen – nur Tatsachen, keine Abstimmung.
- ☐ Ausfälle von IT, Telefonie, Fahrzeugen und Versorgung konkret dokumentieren.
- ☐ Verteidiger über Presse-, Patienten-, Kassen-, KV/KZV-, Kammer- oder Behördenanfragen informieren.
- ☐ Datenschutzvorfall und Meldepflichten nicht eigenmächtig bewerten.
- ☐ Zugänge nur soweit notwendig neu absichern; Veränderungen dokumentieren und mit IT/Verteidigung koordinieren.

In den folgenden Tagen

- ☐ Akteneinsicht und Prüfung von Beschluss, Vollzug, Durchsicht und Beschlagnahmen veranlassen.
- ☐ Rechtsmittel, Herausgabeanträge, Datenbegrenzung oder Löschung verfahrensfremder Kopien prüfen.
- ☐ Abrechnung, Dokumentation, Delegation, Leistungserbringung und Verantwortlichkeiten strukturiert aufarbeiten.
- ☐ Parallelverfahren identifizieren: KV/KZV, Krankenkassen, Kammer, Approbationsbehörde und Zulassungsgremien.
- ☐ Kommunikationsstrategie gegenüber Mitarbeitern, Patienten, Partnern und Öffentlichkeit festlegen.
- ☐ Notbetrieb auswerten und Wiederanlaufplan verbessern.

Warum die Doppelqualifikation zählt

STRAFVERTEIDIGUNG	MEDIZINRECHT
Tatverdacht, Vorsatz, Schaden, Einziehung, Aussage- und Verteidigungsstrategie sowie Rechtmäßigkeit von Durchsuchung, Durchsicht und Beschlagnahme.	EBM/GOÄ/GOZ, Leistungserbringung, Delegation, Dokumentation, Regress, Zulassung, Approbation, Datenschutz und Praxisorganisation.

STRAFVERTEIDIGUNG FÜR ÄRZTE. MEDIZINRECHT INKLUSIVE.

Ihr Strafverteidiger sollte Abrechnung verstehen. Ihr Medizinrechtler sollte verteidigen können. Beides gehört in eine gemeinsame Strategie.

10. Kurzcheckliste zum Aushängen

Am Empfang, im Arztzimmer und in der internen Notfallmappe hinterlegen.

	RUHE BEWAHREN Nicht diskutieren, nicht behindern, keine hektischen Nachrichten.
2	ANWALT ANRUFEN Matthias Klein: 0721 1510 1010
	SCHWEIGEN Keine Angaben zu Abrechnung, Behandlung, Dokumentation oder Zuständigkeiten.
	BESCHLUSS SICHERN Person, Tatvorwurf, Praxis, Wohnung, Fahrzeuge, Zeitraum und Gegenstände prüfen.
	NICHT FREIWILLIG HERAUSGEBEN Förmliche Sicherstellung und vollständige Dokumentation verlangen.
	JEDEN BEAMTEN BEGLEITEN Für jeden Bereich eine eingewiesene Begleitperson.
	DRITTSPHÄREN KENNZEICHNEN Patienten, Familie, Mitbewohner, andere Berufsträger und fremde Fahrzeuge.
	IT-BETRIEB SICHERN Keine Löschung; gezielte Kopie und Rückgabe betriebsnotwendiger Geräte anregen.
	ALLES DOKUMENTIEREN Zeit, Räume, Personen, Daten, Geräte, Fahrzeuge und Ausfallfolgen.
	NICHT UNGEPRÜFT UNTERSCHREIBEN Kopien von Beschluss, Protokoll und Verzeichnis verlangen.

SOFORTHILFE BEI PRAXISDURCHSUCHUNG · 0721 1510 1010

Matthias Klein · Fachanwalt für Strafrecht und Medizinrecht · persönlich · diskret · bundesweit

11. Rechtliche Leitlinien und Hinweise

Organisatorische Ersthilfe – keine abschließende Prüfung des konkreten Beschlusses oder der jeweiligen Verfahrensrolle.

- ☐ Konkreter Tatverdacht: Keine Durchsuchung allein aufgrund vager Anhaltspunkte oder bloßer Vermutungen.
- ☐ Verhältnismäßigkeit: Verdachtsstärke, behaupteter Schaden, Umfang und mildere Mittel sind abzuwägen.
- ☐ Schutz Dritter: In Arztpraxen und privaten Haushalten können hochsensible Daten unbeteiligter Patienten und Familienangehöriger betroffen sein.
- ☐ Zweckbindung: Bei Nichtbeschuldigten müssen gesuchte Spuren oder Gegenstände und der erwartete Auffindeort hinreichend konkretisiert sein.
- ☐ Keine Selbsthilfe: Maßnahmen nicht körperlich verhindern; Einwände dokumentieren und rechtlich prüfen lassen.
- ☐ Kein Automatismus: Eine rechtswidrige Durchsuchung führt nicht automatisch zur Unverwertbarkeit sämtlicher Funde.

Ausgewählte Rechtsgrundlagen und Rechtsprechung

Quelle	Bedeutung für den Notfallplan
§§ 102–110 StPO	Durchsuchung bei Beschuldigten und Dritten, Verfahren, Durchsicht und Dokumentation.
§§ 53, 53a, 97 StPO	Zeugnisverweigerung und Beschlagnahmeschutz bei Berufsgeheimnisträgern; Reichweite einzelfallabhängig.
§ 107 StPO	Auf Verlangen schriftliche Mitteilung über Grund der Durchsuchung und Verzeichnis der in Verwahrung oder Beschlagnahme genommenen Gegenstände.
BVerfG, 21.01.2008 – 2 BvR 1219/07	Arztpraxis: besondere Sorgfalt bei Eingriffsvoraussetzungen und Verhältnismäßigkeit; sensible Patientendaten sind zu berücksichtigen.
BVerfG, 18.02.2008 – 2 BvR 2697/07	Rechtswidrige Durchsuchung führt nicht automatisch zur Rechtswidrigkeit einer Beschlagnahme.
BVerfG, 19.04.2023 – 2 BvR 1844/21	Durchsuchung muss erfolgversprechend und erforderlich sein; mildere Mittel sind zu berücksichtigen.
BSI-Hinweise zur IT-Sicherheitsrichtlinie	Verantwortung, Sicherungsintervalle, getrennte Speicherung und regelmäßige Wiederherstellungstests als Grundlage der Datensicherung.

VORBEREITUNGSEMPFEHLUNG

Den Notfallplan mindestens jährlich im Team besprechen. Rollen, Telefonnummern, Standorte, Fahrzeuge, IT-Dienstleister, Backups und Wiederanlaufverfahren aktualisieren und praktisch testen.

Matthias Klein
Rechtsanwalt · Fachanwalt für Strafrecht · Fachanwalt für Medizinrecht
Telefon 0721 1510 1010 · Karlsruhe · bundesweite Verteidigung