

Checkliste zur Prüfung des Auftragsverarbeitungsvertrags (AVV) für die Datenvernichtung

(Sollte bei der Angebotsanfrage mit übersandt werden,
damit der Dienstleister erkennt was dem Arzt wichtig ist.)

Worauf die Arztpraxis für Ihre Rechtssicherheit achten wird:

Die Beauftragung eines externen Dienstleisters für die Vernichtung von Patientenakten ist eine Form der Auftragsverarbeitung nach Art. 28 DS-GVO. Der Praxisinhaber bleibt dabei immer der "Verantwortliche" und haftet vollumfänglich für die Einhaltung des Datenschutzes und der ärztlichen Schweigepflicht. Diese Checkliste soll helfen, die kritischsten Punkte in einem AVV schnell zu identifizieren, bevor eine Unterschrift geleistet wird.

Zwingend notwendige Punkte im AVV für den Vernichtungsprozess

1. Grundlegende Schutz-Definitionen

| Prüfpunkt | Ja / Nein | Anmerkungen & warum es wichtig ist |
|---|--------------------------|--|
| Ist explizit Schutz- klasse 3 nach DIN 66399 vereinbart? | <input type="checkbox"/> | Das ist nicht verhandelbar. Patientendaten unterliegen der Schweigepflicht (§ 203 StGB) und sind Daten nach Art. 9 DS-GVO. Schutzklasse 2 ist unzureichend und ein klares Warnsignal für einen unseriösen Anbieter. |
| Sind die Sicherheits- stufen für JEDE Mate- rialart konkret be- nannt? | <input type="checkbox"/> | Vage Formulierungen sind wertlos. Der Vertrag muss die Stufen festschreiben (z.B. Papier P-5, Röntgenfilm F-5, Festplatten H-5). Fehlen Angaben, existiert keine vertragliche Grundlage für deren sichere Vernichtung. |
| Sind Gegenstand, Art und Zweck klar defi- niert? | <input type="checkbox"/> | Im Vertrag muss klar "Übernahme und datenschutzkonforme Vernichtung von Patientenakten und -datenträgern gemäß DIN 66399" stehen. |

2. Pflichten und Garantien des Dienstleisters

| Prüfpunkt | Ja / Nein | Anmerkungen & warum es wichtig ist |
|--|--------------------------|---|
| Werden die Mitarbeiter des Haupt-Dienstleisters explizit auf § 203 StGB ver- pflichtet? | <input type="checkbox"/> | Eine allgemeine Verpflichtung zur Vertraulichkeit genügt nicht. Die strafrechtliche Relevanz der ärztlichen Schweigepflicht muss vertraglich auf die Mitarbeiter übertragen werden. |
| Sind die Technischen und Organisatorischen Maß- nahmen (TOMs) ausrei- chend? | <input type="checkbox"/> | Dies beinhaltet die gesamte Logistikkette: Werden abschließbare Sicherheitsbehälter verwendet? Erfolgt der Transport in gesicherten Fahrzeugen? Wie wird der Zugang zum Vernichtungsbereich kontrolliert? |
| Ist eine unverzügliche Mel- depflicht bei Datenschutz- pannen vereinbart? | <input type="checkbox"/> | Der Dienstleister muss sich verpflichten, Ihnen jede Panne sofort zu melden, damit Sie Ihrer eigenen Meldepflicht gegenüber der Aufsichtsbehörde nachkommen können. |

3. Transparenz und Kontrolle (inkl. Subunternehmer)

| Prüfpunkt | Ja / Nein | Anmerkungen & warum es wichtig ist |
|--|--------------------------|--|
| Sind ALLE Subunternehmer namentlich genannt? (Adresse, Land, Aufgabe) | <input type="checkbox"/> | Sie müssen wissen, wer Ihre Daten tatsächlich in den Händen hält (z.B. für Transport, Sortierung). Der Dienstleister darf keine weiteren Subunternehmer ohne Ihre explizite Zustimmung beauftragen. |
| Wird die Verpflichtung auf § 203 StGB lückenlos an ALLE Subunternehmer weitergegeben? | <input type="checkbox"/> | Dies ist ein K.O.-Kriterium. Der AVV muss garantieren, dass auch die Mitarbeiter der Sub-Dienstleister nachweislich auf die ärztliche Schweigepflicht verpflichtet werden. Ihre Verantwortung als Arzt endet nicht am Werkstor Ihres direkten Vertragspartners. |
| Sind Ihre Kontroll- und Auditrechte klar geregelt? | <input type="checkbox"/> | Sie müssen das Recht haben, die Einhaltung der Pflichten zu überprüfen oder durch einen Dritten (z.B. Ihren DSB) überprüfen zu lassen. Ein seriöser Anbieter wird dies durch Zertifikate oder Auditberichte belegen. |

4. Prozessabschluss und Nachweis

| Prüfpunkt | Ja / Nein | Anmerkungen & warum es wichtig ist |
|---|--------------------------|--|
| Wird ein detailliertes Vernichtungsprotokoll pro Auftrag zugesichert? | <input type="checkbox"/> | Dies ist Ihr wichtigster Nachweis für die Erfüllung Ihrer Rechenschaftspflicht. Das Protokoll muss Datum, Behälternummer, Schutzklasse, Sicherheitsstufen und die Bestätigung der Vernichtung enthalten. |

Rote Flaggen – Bei diesen Punkten sollten Sie sofort skeptisch werden:

- Der Anbieter weigert sich, **Schutzklasse 3** in den Vertrag aufzunehmen.
- Es werden nur vage Formulierungen statt konkreter **Sicherheitsstufen nach DIN 66399** verwendet.
- Der Anbieter kann nicht nachweisen, wie die **Verpflichtung auf § 203 StGB an seine Subunternehmer** weitergegeben wird.
- Fehlende Transparenz bei **Subunternehmern**, weil keine Beschreibung der Teilaufgabe gegeben wird.
- Ihre **Kontrollrechte** werden stark eingeschränkt oder mit hohen Kosten verbunden.

Finaler Rat:

Lassen Sie jeden Vertrag vor der Unterzeichnung von Ihrem Datenschutzbeauftragten (DSB) oder einem spezialisierten Rechtsbeistand prüfen. Die Kosten für eine solche Prüfung sind eine Investition, die Sie vor Bußgeldern, Strafverfahren und Reputationsschäden in weitaus größerer Höhe schützen kann.