KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

DARAUF SOLLTEN PRAXEN BEI ANBIETERN VON CLOUDS UND RECHENZENTREN ACHTEN

CHECKLISTE

1. Europäische Datenschutzstandards

- ☐ Ist das Angebot vereinbar mit der Datenschutzgrundverordnung (DSGVO)?
- ☐ Gibt es einen Vertrag zur Auftragsdatenverarbeitung?

2. Standort der gespeicherten Daten

- ☐ Werden die Daten in Deutschland, dem Europäischen Wirtschaftsraum beziehungsweise in einem Land mit Angemessenheitsbeschluss der Europäischen Kommission gespeichert?
- ☐ Gibt es Nachweise für die Einhaltung europäischer Datenschutzstandards?

3. Ende-zu-Ende-Verschlüsselung

- ☐ Werden die Daten Ende-zu-Ende verschlüsselt, das heißt zusätzlich zur Transportverschlüsselung bei der Übertragung, sodass nur in der Praxis auf die entschlüsselten Daten zugegriffen werden kann?
- ☐ Nutzt der Anbieter aktuelle Verschlüsselungsstandards (z. B. AES-256)?

4. Zugriffskontrolle

- ☐ Gibt es eine Mehr-Faktor-Authentifizierung für den Zugang?
- ☐ Können Benutzerrechte individuell vergeben werden?

5. Sicherheitskopien

- ☐ Werden die Daten regelmäßig gesichert, also Backups durchgeführt?
- ☐ Werden die Daten nicht nur auf einem Server gespeichert, sondern redundant an mehreren Serverstandorten?

6. Unterstützung und Dienstleistungsniveau (Support und Service-Level)

- ☐ Gibt es eine Unterstützung rund um die Uhr an sieben Tagen die Woche (24/7-Support)?
- ☐ Werden wichtige Leistungsversprechen auch vertraglich festgehalten (Service-Level-Agreements), zum Beispiel Rufbereitschaft oder eine Problemlösung innerhalb von beispielsweise zwei Stunden?

7. Zertifizierung

- ☐ Kann der Anbieter relevante Zertifikate/Testate vorweisen (z. B. ISO 27001, BSI C5)?

8. Kosten und Anpassungsmöglichkeiten

- ☐ Sind die Kosten für die Datensicherung transparent?
- ☐ Lässt sich der Speicherplatz flexibel anpassen, beispielsweise die Kapazität erhöhen oder auch verringern, ohne dass dies die Leistung beeinträchtigt (Stichwort Skalierbarkeit)?