

# **VA Durchführung einer Bestandsaufnahme der technischen und organisatorischen Infrastruktur zur Umsetzung des DVG, des BDSG und der DSGVO**

## **Übersicht**

Diese VA dient der internen Unterstützung der Verantwortlichen in medizinischen Einrichtungen wie Praxen, Kliniken, MVZ, speziell bei der rechtskonformen Umsetzung der Datenschutz-Rahmenbedingungen (DSGVO, BDSG neu und BvG).

## **Ziel und Zweck**

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zur Durchführung Bestandsaufnahme der technischen und organisatorischen Infrastruktur in geregelten Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und der Sicherstellung der Vollständigkeit und Qualität der Bestandsaufnahme.

## **Anwendungsbereich**

Diese Anweisung gilt für die Ermittlung der technischen und organisatorischen Infrastruktur in allen Bereichen der medizinischen Einrichtung (Praxis, Klinik, MVZ).

Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten, erfasst, verarbeitet, übertragen und gespeichert werden.

## **Verantwortung**

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung/Mitglieder der Leitung (ärztlich und organisatorisch)
- Datenschutz Beauftragte (DSB) und Datenschutz Koordinatoren (DSK)
- Externe Dienstleister, soweit rechtlich geregelt

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

## **Prozesse**

### **Vorbereitung**

Im Rahmen der regelmäßigen Mitarbeiter Besprechungen werden Rollen zur Durchführung der Bestandsaufnahme der technischen und organisatorischen Infrastruktur (TOI) definiert und mit den zuständigen Teammitgliedern abgestimmt. In der Standard-Organisation wird die Bestandsaufnahme durch die/den Datenschutzkoordinator(in) geregelt.

### **Aufgabenverteilung**

Die Bestandsaufnahme umfasst umfangreiche interne und externe Recherchen (IT-Partner/DLO) und muss deshalb im Regelfall auf unterschiedliche Personen/Rollen verteilt werden.

Bei größeren Praxen empfiehlt sich die Erstellung eines strukturierten Projektplans, um die Transparenz der Aufgaben zu gewährleisten.

## **Einzelprozesse**

### **Eingesetzte IT-Produkte allgemein**

- Welche IT-Systeme werden zur Erfassung und Speicherung medizinischer (besonderer) Daten eingesetzt?
- Welche IT-Systeme sind Bestandteil der ärztlichen Dokumentation und unterliegen der gesetzlichen Aufbewahrungsfrist (Fristen siehe Anhang)?
- Wie wird die Verknüpfung zwischen Elektronischer Kartei und Spezialdatenerfassung sichergestellt (Vermeidung falscher Patienten-Zuordnung)?

### **Eingesetzte Hardware (Endgeräte)**

- Welche Hardware wird für die Elektronische Patientenakte eingesetzt?
- Welche Hardware wird für die Spezialdatenerfassung verwendet?
- Welche zusätzliche HW wird zur Dateneingabe eingesetzt (Scanner, Medizintechnik)?

### **Datensicherung**

- Elektronische Patientenakte
- Spezialdatenerfassung

### **Datenschutzrechtliche Kategorisierung der Datenerfassung**

- Datenkategorien der Elektronischen Patientenakte (normal)
- Datenkategorien der Elektronischen Patientenakte (besonders Art. 9 DSGVO)
- Datenkategorien der Spezialdatenerfassung (normal)
- Datenkategorien der Spezialdatenerfassung (besonders Art. 9 DSGVO)
- Datenkategorien der Spezialdatenerfassung (sensibel)

### **Ausgabe von personenbezogenen Daten**

#### **Ausgabe aus der Elektronischen Patientenakte (EPA)**

- An Patienten (elektronisch oder analog)
- An Ärzte und medizinische Einrichtungen
- An Auftragsverarbeiter

- An offizielle Stellen

### **Ausgabe aus Spezialdatenerfassung (SE)**

- An Patienten (elektronisch oder analog)
- An Ärzte und medizinische Einrichtungen
- An Auftragsverarbeiter
- An offizielle Stellen

### **Datenfernkommunikation (z.B. Fernwartung) hier: Datenkategorien**

### **Kontaktdatenverwaltung DSMS relevant (separate Dokumentation: siehe VA)**

### **Ergebnis**

Das Ergebnis der Bestandsaufnahme wird in das Dokument „Bestandsaufnahme zur Infrastruktur“ aufgenommen.

### **Wartung und Aktualisierung**

Mindestens einmal jährlich wird die Bestandsaufnahme für den Jahresbericht aktualisiert. Bei wesentlichen Veränderungen erfolgt ebenfalls eine Aktualisierung:

- Einsatz neuer Server HW
- Erweiterung des IT-Netzwerks
- Anschluss neuer Peripherie
- Erweiterung oder Wechsel der EPA Software
- Erweiterung oder Ersteinsatz von Zusatz-SW (z.B. Studien/Q-Register)
- Neue Anwendungen Datenfernkommunikation (z.B. Telematikinfrastruktur/TI)

Anschließend wird die Risikoanalyse erneuert, um die anschließende Datenschutz-Folgeabschätzung (DSFA) ebenfalls zu aktualisieren.

### **Mitgeltende Dokumente:**

- Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis der BÄK & KBV
- Technische Anlage zu den BÄK/KBV Empfehlungen
- Checkliste zur Bestandaufnahme der Infrastruktur
- Erläuterungen zur Bestandsaufnahme der Infrastruktur
- Richtlinien zur Ermittlung des Verfahrensverzeichnis