

Was verbindet die Medizin und den Datenschutz?

## IHR HANDELN ZUM WOHL DES PATIENTEN!



### GESETZE & RICHTLINIEN DER EU

- Rechtmässigkeit der Datenverarbeitung
  - Gesetzliche Grundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeiten
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung pseudonymer oder anonymisierter Daten
- Verpflichtung zum Schutz der Daten

### KANTONS-GESETZE

### BUNDES-GESETZE

### SPEZIAL-GESETZE

### KIRCHLICHE GESETZE

**«Aegroti salus suprema lex.»**

Das höchste Gesetz ist das Wohl des Patienten.

## DIE DSGVO - WER IST BETROFFEN UND WARUM?

Krankenhäuser, Apotheken, Mediziner aller Fachrichtungen und viele andere Beschäftigte im Gesundheitswesen sind davon betroffen, denn diese bearbeiten äusserst sensible persönliche Informationen (wie Patientenakten, Diagnosen, Krankheitsverläufe, Mitarbeiterdaten und vieles mehr). Da diese Branche mit sogenannten besonders schützenswerten personenbezogenen Daten in Berührung steht, werden die Behörden hier einen Fokus auf die Durchsetzung des Datenschutzes in Bezug auf die DSGVO in der gesamten EU legen. Dies kann und wird bei möglichen Verstössen bedeutendere rechtliche und finanzielle Konsequenzen nach sich ziehen als je zuvor.

## WAS IST ZU TUN?

### 1 AUFZEICHNUNG DER VERARBEITUNGSTÄTIGKEITEN

Für jeden Prozess (z. B. Rezeptbearbeitung, Patientenaufnahme etc.) ist zu dokumentieren, welche Typen von Daten zu welchem Zweck verarbeitet werden, wer sie erhebt, wer darauf zugreift und wo sie wie lange gespeichert werden.

### 2 MITARBEITERSCHULUNGEN

Nachweis, dass alle Mitarbeiter eine regelmässige Schulung in Bezug auf Datenschutz erhalten.

### 3 RISIKOBEWERTUNGEN

Das Risiko für personenbezogene Daten sowie die Wahrscheinlichkeit und Schwere von Schlüsselrisiken müssen jährlich evaluiert werden. Bei Prozessen mit hohem Risiko sind erweiterte Analysen wie die Datenschutzfolgenabschätzung durchzuführen.

### 4 MELDEPFLICHT

Man muss ein detailliertes Protokoll über jede Datenpanne führen und die zuständige Meldestelle innerhalb von 72 Stunden informieren.

### 5 EINWILLIGUNG ZUR VERARBEITUNG

Die Einwilligung zur Gesundheitsdatenerfassung muss transparent formuliert werden, die Zustimmung muss nachweisbar und ein einfacher Widerspruch jederzeit möglich sein.

### 6 AUSKUNFTSRECHT VON INDIVIDUEN

Jeder Patient hat das Recht, über alle Aspekte der Datenerhebung und -verarbeitung informiert zu werden, persönliche Daten zu berichtigen, sie zu löschen, in ihrer Verarbeitung einzuschränken, auf sie zuzugreifen und sie zu erhalten.

Die organisatorischen und technischen Massnahmen in Bezug auf den Datenschutz sind die Grundpfeiler, um mit der DSGVO konform zu gehen. Eine korrekt etablierte und gelebte Governance-Strategie ist die Basis der dafür notwendigen Sicherheitsorganisation.

Wir unterstützen Sie, diese zu etablieren und DSGVO-konform zu agieren.

IS4IT Schweiz AG  
Allmendstrasse 1  
6300 Zug  
Schweiz  
telefon +41 72 00090  
info@is4it.ch  
www.is4it.ch

IS4IT GmbH  
Grünwalder Weg 28b  
82041 Oberhaching  
telefon +49 89 6389848-0  
fax +49 89 6389848-9  
info@is4it.de  
www.is4it.de

IS4IT GmbH & Co. KG  
Franz-Josefs-Kai 49/Top 19  
1010 Wien  
Österreich  
telefon +43 1 227601-0  
info@is4it.at  
www.is4it.at

