# Datenschutz & Datensicherheit

Datenschutz & -sicherheit sind mit dem Image des reinen „Kostentreibers" belastet. Dabei war der Gesundheitssektor im Jahr 2016 die am häufigsten aus dem Internet angegriffene Branche. Der Schutz sensibler Daten wird durch die Datenübertragung außerhalb der eigenen Infrastruktur (Cloud, Geräteanbieter) zunehmend komplizierter. Zudem ist die Erwartungshaltung der Anwender hoch – private Dienste sollen auch am Arbeitsplatz verfügbar sein. Mit Inkrafttreten des IT-Sicherheitsgesetzes 2015 und der EU-Datenschutzverordnung zählt der Gesundheitssektor zu den „kritischen Infrastrukturen" (KRITIS) – damit drohen ab 2018 im Schadensfall empfindliche Bußgelder von bis zu 20 Mio.€.

## IHRE FRAGEN

### Sicherheitsniveau

Wie gut ist Ihr Krankenhaus auf die zweijährig stattfindenden Sicherheitsaudits vorbereitet? Ist Ihre IT bzgl. EU-DS-GVO und IT-Datensicherheitsgesetz auf dem aktuellen Stand und wird das erwartete Mindestsicherheitsniveau erreicht?

### Erfolgsfaktoren

Was sind die Erfolgsfaktoren beim Management von Informationssicherheit?

### Methoden

Wie kann der Sicherheitsprozess vom verantwortlichen Management gesteuert und überwacht werden? Wie sollte eine allgemeine IT-Sicherheitsstrategie aussehen und wie wird sie umgesetzt? Wie werden Sicherheitsziele & Sicherheitsmaßnahmen und mithin eine angemessene Sicherheitsstrategie entwickelt? Wie können Probleme wie Schatten-IT gelöst werden?

### Technische Möglichkeiten

Whitelisting oder Blacklisting (Device/Application)? Wie können Sie sich gegen Cyberattacken schützen?

## UNSERE LÖSUNG

### IT-Security Check

Analyse und Bewertung Ihrer IT-Sicherheit durch unseren detaillierten IT-Security Check. Im Anschluss unterstützen wir Sie bei der Durchführung der erforderlichen Schritte zur Einführung eines ISO-27001-konformen ISMS (Information Security Management System).

### Vorgehen

Festlegung der durch das ISMS abzudeckenden Organisationsbereiche, Prozesse und Datenflüsse in einem Dokumentationsrahmenwerk.

Gemeinsame Identifikation schutzbedürftiger Informationen und Assets.

Durchführung einer detaillierten Schutzbedarfs- und Risikoanalyse.

Entwicklung und Etablierung von Maßnahmen zur Risikobehandlung.

Erstellung und Einführung eines Konzepts zum Messen, Steuern und Überwachen des ISMS.

## IHRE MEHRWERTE

### Transparenz

Überblick über den aktuellen, unternehmensweiten IT-Sicherheitsstatus.

Konzeption bzw. Aktualisierung Ihres IT-Sicherheits- und Datenschutzkonzepts basierend auf einer Risikoeinschätzung Ihres Krankenhauses.

### Qualitätssteigerung

Frühzeitige Risikofeststellung.

Einschätzung des vorhandenen IT-Sicherheitsniveaus.

Empfehlungen für ein optimiertes IT-Sicherheitsniveau.

Implementierung eines Verfahrens für die Definition, Steuerung, Kontrolle und Verbesserung Ihrer Informationssicherheit.

.

**gök Consulting AG** · Berlin · T +49 30 35199670 · www.goek-consulting.de
**Dr. René Rottleb** · M +49 157 70619451 · rene.rottleb@goek-consulting.de
**Michael Schaaf** · M +49 176 10027031 · michael.schaaf@goek-consulting.de

gök CONSULTING