# Der DiGA Leitfaden der GUTcert

Ein integriertes Managementsystem aus
EN ISO 13485 und ISO/IEC 27001 für Digitale
Gesundheitsanwendungen

Ulrich Wegener

© GUT Certifizierungsgesellschaft mbH

# Organisation

- Sprechen: begrenzt auf den Referent
- Schreiben: Fragen richten Sie bitte im Chat direkt an den Organisator – nicht an die gesamte Gruppe
- Hören: Lautstärke bitte individuell einstellen
- Kommunizieren: gerne können Sie im Nachgang des Webinares auf uns zukommen, Kontaktdaten folgen am Ende der Präsentation
- Mehr über DiGA: https://www.gut-cert.de/leistungen/informationssicherheit/diga-zertifizierung

# Die GUTcert - Wer sind wir?

Die GUTcert ist eine international anerkannte Gesellschaft zur Prüfung von

- Managementsystemen
- Produkten
- Personal
- Lieferanten

und bietet Wissenstransfer zu diesen Bereichen an.

Um für ihre Kunden immer auf dem aktuellen Stand zu sein, ist die GUTcert in verschiedenen Gremien aktiv.

(DIN, DAkkS, IHK Berlin, UBA, VNU, UGA, DENEFF, Bitkom, co2ncept plus)

Seit 2015 Mitglied des Global Compact

Global Compact
Netzwerk Deutschland

**Relevante, aktuelle Eckdaten**

- Mehr als 2.000 GUTcert Kunden, 69.000 AFNOR Kunden weltweit
- 8.800.000 € Umsatz 2020
- 68 Mitarbeiter
- 150 Auditoren und 30 Fachexperten (D), 1.900 weltweit

# Leistungen der GUTcert

## Zertifizierungen

ISO 9001
ISO 14001
ISO/IEC 27001
- ITSK Netze und Energieanlagen
- KRITIS § 8a (3) BSIG

ISO 45001
- SCL Safety Culture Ladder (akkred. von NEN)

AZAV
ISO 50001
- Testierung nach SpaEfV

ISO 55001 Asset Management (nicht akkr.)

## Verifizierungen

Emissionen & Zuteilungsanträge (ETS)
Carbon Footprint / ISO 14064
Klimaneutralität (nicht akkreditiert)
ACA Airport Carbon Accreditation

## Validierung

EMAS nach DAU

## Im Verbund mit Afnor

IRIS Rev 03 (ISO TS 22163)
IATF 16949
AS 9100

## Nachhaltigkeitsstandards

Nachhaltigkeits-Reporting (GRI/ DNK)
ASI Aluminium Stewardship Initiative
RS ResponsibleSteel
ISCC / REDcert / RSPO
ISO 20121 Nachhaltiges Eventmanagement

## Weitere Prüfungen

AwSV-Anlagenprüfung
Kreislaufwirtschaft (z.B. EfB, GewAbfV)
EEG 2009 / 2012 / 2014 / 2017 / 2021
Biomethaneinspeisung
Grünstrom
Herkunftsnachweise (HkN)
EcoStep

## GUTcert Akademie

Auditoren- und Beauftragtenschulungen
Fachkundelehrgänge
Inhouse-Schulungen
Customized E-Learning-Programme

## Berlin Cert

**Benannte Stelle für**
Richtlinie 93 / 42 / EWG
Systeme (Anhänge II, V, VI)
Produkte (Anhang IV)

**Prüflabor**
Elektrische und mechanische Prüfungen von Medizinprodukten
Filterprüfungen an Schutzmasken

**Zertifizierstelle für**
ISO 13485

# Programm Teil 1

Der DiGA Leitfaden der GUTcert

- Übersicht der Ausgangssituation
- Externe Anforderungen und deren Umsetzung im DiGA Leitfaden
- Vorstellung der vier Phasen – Integration ISO/IEC 27001 in ein QM System EN 13485
- Sicherheitsanforderungen, Datenschutz

# Programm Teil 2

Erfahrungsaustausch - Diskussion

- Umsetzung ISO 27001 bei DiGA Herstellern
- Schritt für Schritt
- Was ist zu beachten? Risikoanalyse SoA

# Ausgangssituation

„Eine Digitale Gesundheitsanwendung ist die APP auf Rezept“
Jens Spahn BMfG (2018)

- Rechtsgrundlage:
  - Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation ändert u. a. SGB V § 33a (Geburt der DiGA)
  - Hinweise zu  Datenschutz/Datensicherheit in SGB V § 33a
  - „Gesundheits-Apps“ bekommt man auch ohne Rezept!
    → keine DiGA

# Externe Anforderungen - die DiGA ein Medizinprodukt

Die DiGA ist per gesetzl. Definition ein Medizinprodukt

- Der Hersteller eines Medizinproduktes muss nach EN ISO 13485 zertifiziert sein.
- Jedes Medizinprodukt hat eine Medizinprodukte-Akte, die Technische Dokumentation

 © GUT Certifizierungsgesellschaft mbH 

# Externe Anforderungen Cyber-Sicherheit und Datenschutz

Näheres zu den Eigenschaften der DiGA regelt die DiGAV, gefordert wird:

- Management der IT-Sicherheit -> ISMS
- IT-Sicherheit -> Stand der Technik wird durch BSI festgelegt
- Datenschutz

Im Anhang zu DiGAV gibt es eine Tabelle, nach der die Hersteller gegenüber dem BfArM erklären, dass sie die Anforderungen der einzelnen DiGAV-Aspekte erfüllen.

# Fristen nach DiGAV (Stand 1. Oktober 2021)

Nach Änderung durch:
Erste Verordnung zur Änderung der Digitale Gesundheitsanwendungen-VO

| | 01.04.2022 | 01.08.2022 | 01.01.2023 | 01.04.2023 |
|---|---|---|---|---|
| ISMS | 27001 oder BSI 200 Zertifikat | | | |
| Datensicherheit | | BSI Update SdT (01.06.2022) | Vorgaben des BSI § 139e Abs. 10 SGB V | |
| Interoperabilität | | Antrag ab Datum → InterOp. ePA | InterOp. ePA Schnittstelle Gematik | |
| Datenschutz | | | | Vorgaben des BfArM § 139e Abs. 11 SGB V |

# Externe Anforderungen - das ISMS zur DiGA

Die DiGAV lässt zwei Möglichkeiten:

- Zertifizierung nach ISO/IEC 27001
- BSI Grundschutz 200

Idee von GUTCert und Berlin Cert

- Integriertes Managementsystem aus
  - QM nach EN ISO 13485 und
  - ISMS nach ISO/IEC 27001 mit Elementen aus EN ISO 27799

# Leitfaden und Checkliste zur DiGA

- Leitfaden für die Implementierung
- Checkliste enthält die notwendigen Controls aus 27001 und 27799
- Cross-Referenz Anforderungen 13485 auf Controls (was muss wo hin)

Ebenfalls Bestandteil:

- Aktueller Katalog der IG-NB zur IT-Sicherheit

# Leitfaden Stufenmodell

- Der Leitfaden umfasst vier Phasen
  - Phase I
    Anwendungsbereich, Aufbauorganisation
  - Phase II
    Integration der Anforderungen der ISO/IEC 27001
  - Phase III
    Betrieb des ISMS
  - Phase VI
    Zertifizierung

# Sicherheitsanforderungen

- Aktueller Katalog der IG-NB zur IT-Sicherheit
- BSI TR-03161 Sicherheitsanforderungen an DiGA
- Anforderungen aus Anhang zur DiGAV
  - Datenschutz 1-40
  - Datensicherheit 1-37 (Basis) und
  - Datensicherheit 1-9 (Hoch)

# Datenschutzanforderungen

- Anforderungen § 4 Datenschutz und Datensicherheit
- Anforderungen aus Anhang zur DiGAV
  - Datenschutz 1-40
- SGB V § 139e Absatz 11
  - Prüfkriterien den BfArM
  - Zertifikat nach DSGVO Art. 42

 © GUT Certifizierungsgesellschaft mbH 

# Teil II

## Erfahrungsaustausch – Diskussion

# Ausschnitt Leitfaden (SoA)



## Erklärung zur Anwendbarkeit / Statement of Applicability (SoA)

Wozu brauche ich eine SoA, wenn ich doch eine komplette Managementsystem-Dokumentation habe, in der ich auch Aussagen zum Geltungsbereich meines Systems aufgeschrieben habe?

Der Grund dafür liegt in der besonderen Struktur der ISO/IEC 27001 – im Vergleich zu den anderen Managementsystem-Normen.

Die ISO/IEC 27001 enthält zunächst alle Elemente, die auch andere Systeme (z.B. nach ISO 13485) enthalten. Diese basieren auf der sogenannten High Level Structure, die die ISO als Grundlage für alle Managementsystem-Normen definiert hat.

Der nächste Schritt für alle Anwender einer derartigen Norm ist es nun, Maßnahmen zu definieren, mit denen die Ziele der Norm erreicht werden können und dafür interne Prozesse und Regelungen aufzustellen. Für die ISO/IEC 27001 übernimmt der Normengeber selber den ersten Schritt, indem im Anhang A insgesamt 114 Maßnahmen festlegt sind, die in jedem zertifizierten ISMS berücksichtigt werden müssen. Natürlich kann es dabei vorkommen, dass einzelne dieser Maßnahmen keine Anwendung finden

# Ausschnitt Checkliste (verschlüsselte Datensicherung)

| | | |
|---|---|---|
| A.12.3.1 | Werden Sicherheitskopien von Information, Software und Systemabbildern entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet?<br>[...]<br>Werden die personenbezogene Gesundheitsdaten zum Schutz ihrer Vertraulichkeit in einem verschlüsselten Format gesichert?<br>[Die DIN EN ISO 27799 geht als allg. anerkannte Regel der Technik hier über die Forderungen der DiGAV hinaus.] | DIN EN ISO 27799<br>12.3.1<br>DiGAV |

# Was ist wichtig im Audit?

- Der Geltungsbereich der ISO/IEC 27001 ist im Optimalfall genau so groß, wie der der EN ISO 13485, ggf. größer, er kann nie kleiner sein als der Bereich der DiGA.
- Wurde die EN ISO 27799 identifiziert?
  - Gesundheitsdaten des Patienten sind als Werte zu identifizieren.
  - Die DiGAV fordert die Verschlüsselung der Datensicherung nur in bestimmten Fällen, die EN ISO 27799 bei Gesundheitsdaten immer!

# Was ist wichtig im Audit?

- Die im CyberSecurity Leitfaden der IG-NB genannten Anforderungen müssen identifiziert sein (das gilt bereits für das Medizinprodukt).
  - BSI TR-03161 Sicherheitsanforderungen an DiGA (auch Prüfung → BSI Gesetz, derzeit wird nicht geprüft).
- Die DiGAV fordert Pen-Tests der Infrastruktur, hier muss bewertendes und planendes Handeln im ISMS sichtbar sein.
- Es muss sichergestellt sein, dass das ISMS auch auf die „Technische Dokumentation“ der DiGA wirkt.

# Für alle weitere Fragen

**Bozena Jakubowska**
ISMS Produkt Manager
bozena.jakubowska@gut-cert.de
+49 30 2332021-65

**Ulrich Wegener**
Auditor GUTcert & BERLIN Cert
ulrich.wegener@gut-cert.de
uwegener@berlincert.de
+49 30 2332021-26

 © GUT Certifizierungsgesellschaft mbH

Herzlichen Dank,

für den anregenden Austausch.