TeleTrusT
Pioneers in IT security.

IT-Sicherheitsrechtstag 2018

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Berlin, 25.10.2018

Akkreditierung und Zertifizierung nach DSGVO

Neno Rieger / Nico Behrendt

GUT Certifizierungsgesellschaft mbH

Akkreditierung und Zertifizierung nach DSGVO

Zertifizierung ist Vertrauenssache:
am besten GUTcert

Teletrust IT-Sicherheitsrechtstag 2018

Die GUTcert - Wer sind wir?

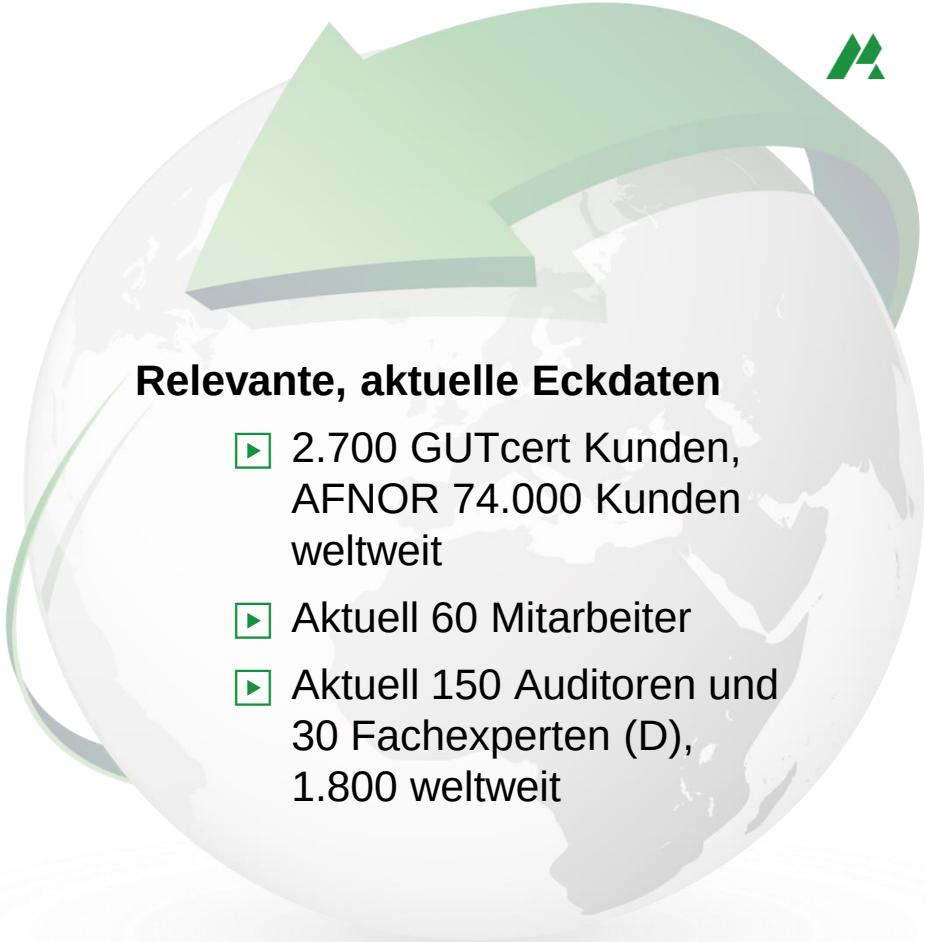
Die GUTcert ist eine international anerkannte Gesellschaft zur Prüfung von

- Managementsystemen
- Produkten
- Personal
- Lieferanten

und bietet Wissenstransfer zu diesen Bereichen an.

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

(DIN, DAkkS, IHK Berlin, UBA, VNU, UGA, AG ZPA, ENERWA)



Relevante, aktuelle Eckdaten

- 2.700 GUTcert Kunden, AFNOR 74.000 Kunden weltweit
- Aktuell 60 Mitarbeiter
- Aktuell 150 Auditoren und 30 Fachexperten (D), 1.800 weltweit

GUTcert und AFNOR - Weltweit vertreten

2008 wird die GUTcert Teil der AFNOR Groupe - „Association Francaise de Normalisation“ und Mitglied der ISO.

Als Teil dieses Netzwerks

- greift die GUTcert heute weltweit auf mehr als 1.800 Auditoren aus über 90 Ländern zurück
- ist die GUTcert verstärkt international tätig
- Bietet die GUTcert Zertifizierungen über die volle Bandbreite von Managementsystemen an – auch integriert!

Unsere Leistungen

DAkkS Deutsche Akkreditierungsstelle

Zertifizierungen

ISO 9001
ISO 14001
BS OHSAS / ISO 45001
AZAV
ISO 22000 (-FSSC)
ISO 27001 / ITSK
ISO 50001
Testierung nach SpaEfV:
Alternative Systeme
Energieaudit nach DIN EN 16247

Im Verbund mit **AFNOR** u.a.
ISO TS 22163 (IRIS Rev. 03)
IATF 16949
AS 9100

und **EMAS** nach DAU

DAkkS Deutsche Akkreditierungsstelle

Verifizierungen

Emissionsberichte (ETS)
Carbon Footprint nach ISO 14064

Prüfungen

ISCC / REDcert / RSPO
EEG 2009 / 2012 / 2014 / 2017
Biomethaneinspeisung
Herkunftsnachweise (HkN)

Entsorgungsfachbetriebe

Datenschutz (DSGVO)

Asset Management ISO 55001

Stand der Nachhaltigen Entwicklung (DNK und GRI)

Berlin Cert ist

ZLG **Benannte Stelle für**

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

DAkkS Deutsche Akkreditierungsstelle **Zertifizierstelle für**
ISO 13485

Prüflabor für Medizinprodukte

GUTcert Akademie

UM / QM / EnMS / ISMS u.a.
Auditoren- und Beauftragtenschulungen

Inhouse-Schulungen

Customized
E-Learning-Programme

Zertifizierung = Dienstleistung!

- Zertifizierungen sollen die **Effizienz, die Wirtschaftlichkeit und die Sicherheit** unserer Kunden verbessern

- Wir verstehen Normen als konzentriertes Expertenwissen, das bereitgestellt wird, um formale Anforderungen zu erfüllen - **Nicht die Form einer Tätigkeit entscheidet über das Produkt, sondern der Inhalt!**

- Normenforderungen dürfen und sollen zum Nutzen einer Organisation interpretiert werden.

DAkkS Akkreditierung

Wer benötigt eine Akkreditierung?

- nach Art. 42 Abs. 5 EU-DSGVO:

  alle Zertifizierungsstellen die „datenschutzspezifische“ Zertifizierungsleistungen, Gütesiegel oder Prüfzeichen jeder Art anbieten wollen und mit denen ausdrücklich oder mittelbar die Konformität mit datenschutzrechtlichen Anforderungen der Grundverordnung bestätigt wird

- nach Art. 41 Abs. 2 EU-DSGVO:

  Überwachungsstellen

DAkkS Akkreditierung

Wer als Zertifizierungsstelle

- ohne eine Akkreditierung der DAkkS,
- ohne Zulassung einer zuständigen Aufsichtsbehörde und/oder
- auf Grundlage „nicht genehmigter Kriterien“,

Zertifikate ausgibt, welche direkt oder indirekt die „Konformität“ mit den Anforderungen der Grundverordnung bestätigen,

- verstößt gegen die Grundverordnung und setzt sich hohen rechtlichen Risiken aus,
- verstößt wettbewerbsrechtlich gegen Nr. 2 des Anhangs zu §3 Abs. 3 UWG („die Verwendung von Gütezeichen, Qualitätskennzeichen oder Ähnlichem ohne die erforderliche Genehmigung“).

DAkkS Akkreditierung

- Gem. §43 DS-GVO (Zertifizierungsstellen) & §39 BDSG-Neu (Akkreditierung)

- 1. Stufe: Akkreditierung durch DAkkS - Kompetenzfeststellung (“fachliches Können”)
- 2. Stufe: Befugniserteilung durch Behörde - Erlaubnis (“rechtliches Dürfen”)
- Tätigkeit der Zertifizierungsstelle in diesem Bereich am Markt
  - Gültigkeit nur in Deutschland
- Die Besonderheit im Datenschutz ist die Genehmigung von Zertifizierungskriterien und Anforderungen zur Akkreditierung

Struktur des Akkreditierungssystems

- **Level 3:**
  - Genehmigte „Anforderungen“ Akkreditierung: ISO 17065
- **Level 4:**
  - Standards zur Evaluierung wie: ISO 15408, Standard-Datenschutzmodell (SDM)
  - Genehmigte Kriterien für Konformitätsbewertungsprogramme ISO 17065, ISO 17030
- **Level 5:**
  - Anforderungen an den „Gegenstand“ der Bewertung (Verantwortlicher, Auftragsverarbeiter oder Produkt, Verfahren, Prozess sind nicht Gegenstand von DAkkS-Regeln.)
  - Diese Anforderungen folgen abschließend als „grundlegende Sicherheitsziele“ aus der DSGVO

Konformitätsbewertungsprogramme

- Sehr wahrscheinlich die Entwicklung verschiedener Programme
- Unter dem Dach der VAZ wird ein solches Programm entwickelt
  - Breite Basis an Zertifizierungsstellen (z.B. DEKRA, VdS, PüG)
- **Basis der Zertifizierung:**
  - Verarbeitungsvorgänge die in Prozessen erbracht werden
  - und gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter
  - die Konformität mit den Vorgaben der DSGVO unmittelbar oder mittelbar bestätigen.

Zertifizierung

- Dokumentenprüfung + Vor-Ort wie bei ISO 17001 (noch nicht entschieden)
- Prüfkriterien sind die Inhalte der DSGVO & BDSG-Neu
  - Verfahren, dass der Zustand auch dauerhaft erhalten bleibt
- Überprüfung der TOMs
  - Organisatorische: Handlungsanweisungen, Verfahrens- & Vorgehensweisen
  - Technische: “physischer” Schutz - Wie sicher sind die Daten
  - Bereits in der ISO 27001 (ISMS) erhalten
- Umfang wird ähnlich zur ISO 27001

Personalkompetenz

- Das für die Evaluierung und Entscheidung verantwortliche Personal muss:
  - Kenntnisse und Erfahrungen im technischen und organisatorischen Datenschutz haben und nachweisen können
  - Rechtliche als auch technische Fachkunde besitzen
- Rechtlich:
  - 1. mindestens achtsemestriges Studium der Rechtswissenschaften an einer deutschen staatlichen oder staatlich anerkannten Hochschule und den akademischen Grad Master (LL.M.) oder das Juristische Staatsexamen
  - 2. Für Entscheider: Berufserfahrung von mind. fünf Jahren im Datenschutzrecht
  - 3. Für Evaluatoren: Berufserfahrung von mind. zwei Jahren im Datenschutzrecht & Kenntnisse sowie Erfahrungen in Prüfverfahren (z.B. Zertifizierungen/Auditierungen)

Aussicht

- Bis Ende des Jahres Einreichung des Programms
- Akkreditierung voraussichtlich 1. Quartal 2019
- Markt abhängig von:
  - Entwicklung der Programme
  - Umfang der Zertifizierungen
  - Politischen Entscheidungen

Ihr Referent

Neno Rieger

eMail: neno.rieger@gut-cert.de

Telefon: 030 2332021-67

Vielen Dank für Ihre Aufmerksamkeit