# TeleTrusT "IT-Sicherheitsrechtstag 2022"

**Berlin, 21.09.2022**

# Zertifizierungen gemäß Art. 42 DSGVO aus Sicht einer Zertifizierungsstelle

**Alisha Gühr, datenschutz cert GmbH**

# Agenda

- Vorstellung datenschutz cert GmbH
- Aktueller Stand Akkreditierung von Art. 42 Zertifikaten
- Vorteile
- Unser Ansatz
- Zertifizierungsprozess

Quelle: https://www.dakks.de/de/akkreditierungsfaehige-programme.html, Stand 19.09.2022

# datenschutz cert GmbH

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Wir prüfen und zertifizieren Datenschutz und Informationssicherheit.

# Unsere Akkreditierungen und Anerkennungen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

**Deutsche Akkreditierungsstelle (DAkkS)**

- ISO/IEC 27001
- IT-Sicherheitskatalog
- eIDAS-Konformitätsbewertungsstelle

**Bundesnetzagentur**

- eIDAS-Zertifizierungsstelle

**EuroPriSe (2B Advice GmbH)**

- Lizensierte Experten für Datenschutz-Gütesiegel

**Gematik**

- Sicherheitsgutachten

**Bundesamt für Sicherheit in der Informationstechnik (BSI)**

- IT-Grundschutz /Prüfbegleitung
- IS-Revision
- IT-Sicherheitsdienstleister (Pentests)
- Prüfstelle für IT-Sicherheit (TR-ESOR)
- TR 03145 „Secure CA Operation“
- TR 03109-6 „Smart Meter Gateway Administration“

**PTB**

- Spielautomaten

**IT-Sicherheitscluster e.V.**

- Zertifizierungsstelle für CISIS12/ISIS12

# Aktueller Sachstand Akkreditierung

- datenschutz cert GmbH

## Programme im Bereich Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen

Akkreditierung nach DIN EN ISO/IEC 17065

Certification of fire protection systems for wind turbines (DNVGL-SE-077:2015-03); Subsea power cables (DNVGL-ST-0359:2016-06); Loads and site conditions for wind turbines (DNVGL.ST-0437:2016-xx) ›

DS-GVO | European Data Protection Certification (AUDITOR) ›

DS-GVO | Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern gemäß DSGVO nach der EuroPriSe-Methode ›

DS-GVO | Konformitätsbewertungsprogramm zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO („information privacy standard“) ›

Quelle: https://www.dakks.de/de/akkreditierungsfaehige-programme.html, Stand 19.09.2022

# Aktueller Sachstand Akkreditierung



**Entwicklung**

- Erstellung Konformitätsbewertungsprogramm (KBP) mit Kriterien

**Akkreditierung**

- Abnahme von Programm mit Kriterien durch DAkkS, zuständigem LfDI und EDSA
- Akkreditierung von Zertifizierungsstellen durch DAkkS und zuständigem LfDI

**Anwendung**

- Erteilung von Zertifikaten durch Zertifizierungsstellen

# Warum ein Datenschutzzertifikat ?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

## Was sind Ihre Vorteile?

- ✓ Umsetzung von Rechenschaftspflichten / Compliance
- ✓ Minimierung von Risiken bei Datenpannen
- ✓ Besserer Datenschutz
- ✓ Besseres Image
- ✓ Marktzutrittsvoraussetzung
- ✓ Wettbewerbsvorteil

# Art. 42 DSGVO Zertifikat vs. ISO 27701

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

## Art. 42 DSGVO Zertifikat

- ✓ Zertifizierungsverfahren für Verarbeitungsvorgänge
- ✓ kein Produkt / kein Unternehmen / keine Personen / kein Managementsystem
- ✓ Aussagen über die Datenschutzkonformität

## ISO 27701

- ✓ Zertifizierung des Datenschutzmanagements
- ✓ kein Produkt / keine Dienstleistungen, keine Personen
- ✓ Aussage über die Funktionsfähigkeit des Datenschutzmanagementsystems
- ✓ Baut auf Informationssicherheitsmanagementsystem auf

# Unser Ansatz für ein DSGVO Zertifikat

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

„information privacy standard“©

- generisch: ein Programm für alle
- 3 Jahre Gültigkeit, jährliche Überwachung
- Gegenstand: IT-gestützte Verarbeitung von personenbezogenen Daten durch Verantwortliche und Auftragsverarbeitern

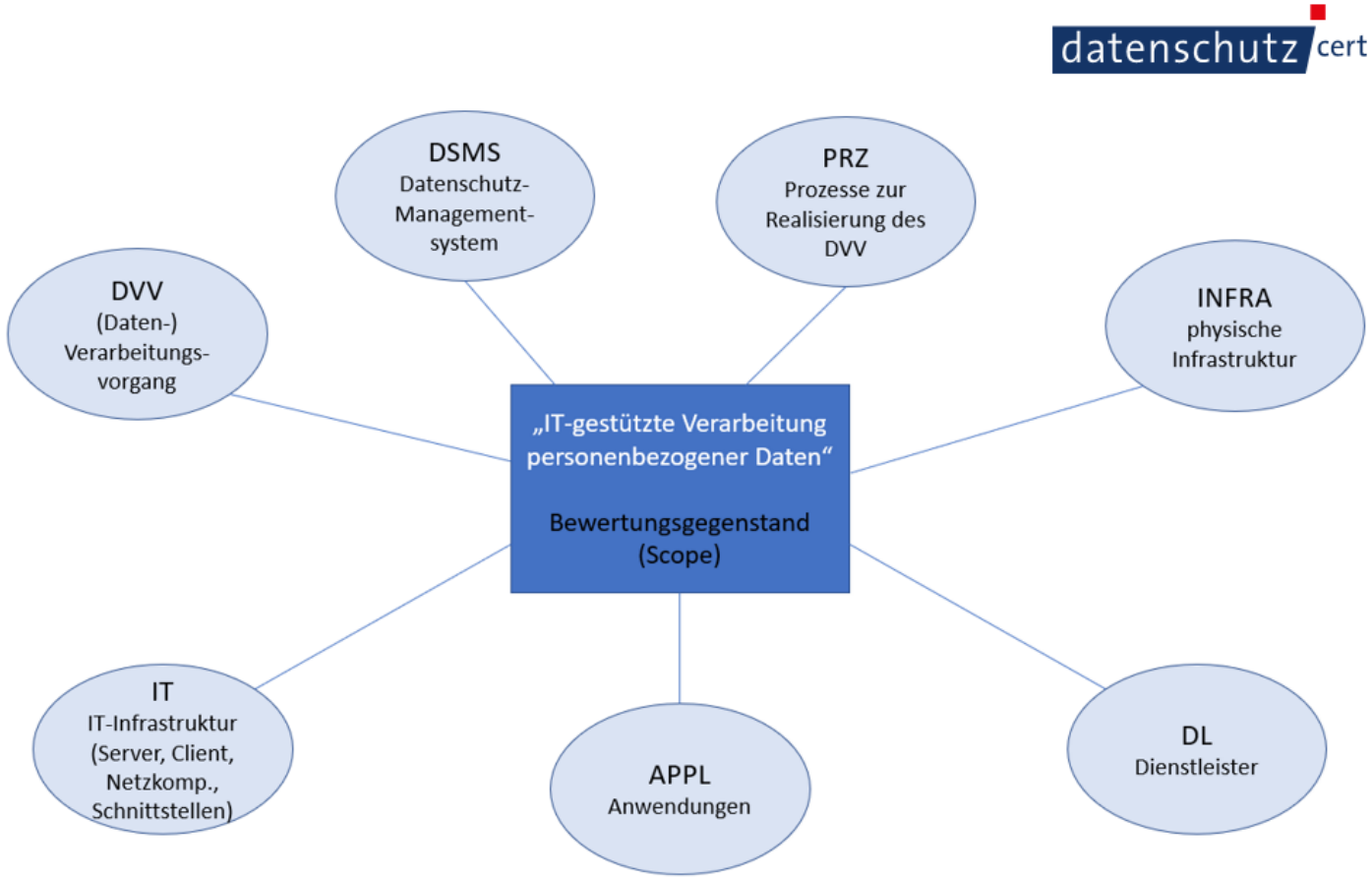
# Unser Ansatz für ein DSGVO Zertifikat

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Zertifiziert werden können Bewertungsgegenstände in verschiedenen Branchen, Bereichen oder Sektoren, beispielsweise:

- ✓ Banken und Versicherungen;
- ✓ Energie- und Wasserversorgung;
- ✓ Gesundheits- und Sozialwesen;
- ✓ Industrie und Handel;
- ✓ Marketing und Werbung;
- ✓ EDV, Informationstechnologie und Telekommunikation;
- ✓ Institute und Verbände;
- ✓ Kultureinrichtungen;
- ✓ Öffentliche Stellen und öffentliche Verwaltung;
- ✓ Transport, Verkehr und Logistik;
- ✓ Kirchen;
- ✓ Schule, Bildung und Wissenschaft;
- ✓ Ernährung.

# Gegenstand der Zertifizierung



# Zertifizierungsprozess

**Angebot**

- Antrag
- Angebotserstellung
- Abstimmung Zeitplanung
- Abstimmung des Zertifizierungsgegenstandes

**Evaluierung**

- Vorbereitung / Auftakt
- Einreichung Dokumente und Nachweise
- Evaluierung (Basisprüfung und Evaluation mit verschiedene Methoden)
- Berichterstellung

**Zertifizierung**

- Erteilung des Zertifikats
- Übermittlung Urkunde und Bericht
- Gültigkeit 3 Jahre bei jährlicher Überwachung
- Listung im Verzeichnis

# Zertifizierungsprozess – erforderliche Informationen

- Beschreibung des Zertifizierungsgegenstandes
  - z.B. Datenverarbeitungsvorgang, Datenarten, relevante Standorte, Subdienstleister, etc.
- Umsetzungsbeschreibung mit Nachweisen
- Ansprechpartner (für remote und on-site Evaluation)
- Testzugänge

# Erforderliche Informationen – Einzureichende Unterlagen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Handelsregisterauszug
- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutzerklärung / Informationen
- Konfigurationsnachweise
- Mustertexte Verträge und AGB / Einwilligungen
- Nachweise über bestehende anerkennbare Zertifikat z.B. ISO/IEC 27001
- Verträge zur Auftragsverarbeitung
- Dokumentation der technischen und organisatorischen Maßnahmen für alle relevanten Standorte
- Netzwerkplan
- Datenschutzfolgenabschätzung und Risikoanalyse
- Bestellurkunde, Fachkundenachweise und Meldebescheinigung bDSB
- Muster Verpflichtungserklärung zur Einhaltung des Datenschutzes für Beschäftigte
- Schulungsnachweise zum Datenschutz und zur Datensicherheit für Beschäftigte
- Richtlinie zum Umgang mit Datenschutzverletzungen
- Richtlinie zum Umgang mit Betroffenenanfragen
- Ggf. Datenschutzhandbuch, Benutzerhandbuch

# Kriterien

- P.1 Zulässigkeit der Datenverarbeitung
- P.2 Grundsätze
- P.3 Pflichten des Kunden
- P.4 Auftragsverarbeitung
- P.5 Technisch-organisatorische Maßnahmen
- P.6 Datenschutz-Management
- P.7 Datenverarbeitung außerhalb der EU
- P.8 Betroffenenrechte
- P.9 Förderung des Datenschutzes

# Typische Fallstricke

- Abgrenzung Zertifizierungsgegenstand, z.B. Support
- Unabhängigkeit, etwa durch Beratungsbedarf
- Rechtsgrundlagen
- Unrechtmäßiger Drittstaatenbezug
- Fehlende Ressourcen / Vorbereitung
- Dokumentation von Prozessen
- Abweichungen während der Evaluierung
  - Problem: keine Nebenabweichungen möglich.

# Kosten einer Zertifizierung

- Abhängig von zahlreichen Faktoren
  - etwa Umfang des Gegenstandes
  - Menge der Verarbeitungen
  - Größe des Unternehmens
  - Anzahl und Ort der Standorte
  - bestehende Zertifikate
  - etc.

# Weitere Informationen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

## Ihre Ansprechpartner:

datenschutz cert


***Alisha Gühr***
datenschutz cert GmbH
**T** +49 (0) 421 69 66 32-50
**E-Mail** aguehr@datenschutz-cert.de

**Dr. Irene Karper**
datenschutz cert GmbH
**T** +49 (0) 421 69 66 32-50
**E-Mail** ikarper@datenschutz-cert.de

**Dr. Sönke Maseberg**
datenschutz cert GmbH
**T** +49 (0) 421 69 66 32-50
**E-Mail** smaseberg@datenschutz-cert.de

**Katja Starke**
datenschutz cert GmbH
**T** +49 (0) 069 87 00 78 35 84
**E-Mail** starke@datenschutz-cert.de


DSGVO
information
privacy
standard

Weiterte Informationen unter https://www.datenschutz-cert.de/leistungen/dsgvo-zertifizierung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

# Haben Sie Fragen?