Datenschutz-Zertifizierung

Nur sicher mit dem Siegel?

Vortrag ZT Oliver Pönisch

Einordnung Datenschutz-Zertifizierungen

ZIVILTECHNIKER OLIVER PÖNISCH

ZTOP

Private (akkreditierte) Zertifizierungen

gesetzlich (akkreditierten) Zertifizierungen

Begutachtung / Attestierung

Individuelle Arbeiten, Frameworks, Prüfungsstandards, **ZT Siegel**

(Akkreditierte) Zertifizierungen

ISO 27701

DSGVO Art 42

Self-/Foreign-Assessments

Frei Verfügbar, Consulting

Einordnung Datenschutz-Zertifizierungen

ZIVILTECHNIKER OLIVER PÖNISCH

Maßgeblich ist:
- Prüfungsinhalt
  (Relevanz zur Rechtsnorm)
- Prüfungstiefe
- Vergleichbarkeit von Ergebnissen

DSGVO Art 42

ISO 27701
ZT Siegel

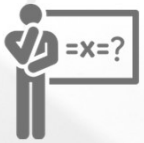
Begutachtung / Attestierung

(Akkreditierte) Zertifizierungen

Aussagekraft der Zertifizierung

Self-/Foreign-Assessments

Frei Verfügbar, Consulting



Welche Zertifizierung ist für mich am besten?

Einordnung Datenschutz-Zertifizieru

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

ZIVILTECHNIKER OLIVER PÖNISCH

DSGVO Art. 42 Zertifizierungen	ISO 27701 und -2	ZT Siegel
(Nur) Verarbeitungen bzw. Teile davon	Keine eigenständige Norm – Erweiterung zu ISMS	▷ Datenschutz-Management-Prozesse ▷ Verarbeitungen ▷ TOMs ▷ rechtliche Aspekte
keine Datenschutz-Management-Prozesse	▷ **keine** rechtlichen Aspekte, ▷ **keine** Verarbeitungen oder Teile davon	Als Attestierung mit fixen Grundgerüst und vereinbarten Zielen **volle Flexibilität**
Nachweis nach DSGVO unter Behördlicher Aufsicht	**Nachweis der Informationssicherheit** (mit Datenschutzaspekten)	**Nachweis der DSGVO** durch Zeugnis einer mit öffentlichem Glauben versehenen Person
Qualitätssicherung durch **behördliche Akkreditierung**	Qualitätssicherung durch **Zertifizierungskörper**	Qualitätssicherung durch **Bundesministerium für Justiz**
Wirkung … ▷ Verantwortlichkeit, ▷ TOMs, ▷ Geeignete Garantien für Datentransfers ▷ Gebührende Berücksichtigung bei Geldbußen	**Wirkung …** ▷ Verantwortlichkeit, ▷ TOMs, ▷ Gebührende Berücksichtigung bei Geldbußen	**Wirkung …** ▷ Verantwortlichkeit, ▷ TOMs, ▷ Geeignete Garantien für Datentransfers, ▷ Gebührende Berücksichtigung bei Geldbußen

ZT DS Zertifizierung Prüfung

- Drei wesentliche Eckpunkte
  - Aspekte der IT-Compliance
    - Technik ➔ IT-Ziviltechniker
    - Prozesse ➔ IT-Ziviltechniker
    - Recht ➔ Rechtsanwaltskanzlei
  - Risikoperspektive
    - Klassische IT Risk Perspektive
    - „Neue“ Data Privacy Risk Perspektive
    - Compliance Risk Perspektive
  - Kontinuität
    - Zertifizierung wird als Teil eines PDCA Zyklus verstanden

ZT DS Zertifizierung Prüfung

ZIVILTECHNIKER OLIVER PÖNISCH

- Primären Anforderungen
  - „Erfüllt das Unternehmen alle formalen Anforderungen?“
  - Bewertung: erfüllt / nicht erfüllt
- Sekundäre Anforderungen
  - „Verfügt das Unternehmen über Prozesse und Maßnahmen zur Erfüllung/Aufrechterhaltung von formalen Anforderungen und sind diese effektiv?“
  - Bewertung: Reifegrad
- Basis einer *Data Privacy Governance*
  - „Ist das Unternehmen in der Lage unabhängig von seinen Akteuren formale Anforderungen und deren Prozesse betreiben zu können?“
  - Bewertung: Reifegrad

Framework abgeleitet aus der DSGVO (~ 30 *Kategorien)*

Vorgehensweise und Aufbau basieren auf Normen zu Konformitätsbewertung

Das Framework basiert auf internationalen bedeutenden Standards: ISO 27000+, 9000, 14000, 17000; CARPA; NOREA, EDPB Guidelines; OWASP …

Ablauf und Aufrechterhaltung der ZT DS Zertifizierung

ZIVILTECHNIKER OLIVER PÖNISCH

Scope
- Prüfweite / -tiefe / -umfang
- Zielsetzung und Hintergrund
- ggf. Priorisierung
- Erstellung des Auditprogrammes


Auditauftrag


Auditprogramm

Erst-Begutachtung
- Schaffung eines Gesamt(System)Überblicks
- Sicherstellung primärer Anforderungen
- Proof-of-Concept / -Design ggf. mit Stichproben
- Erstellung eines *Compliance-Risk-Reports (CRR)*
- Erstellung des Basis-Gutachtens zur Zertifizierung


Auditplan


CRR


α Gutachten

Zertifizierung (Überwachung)
- ggf. Überprüfung Remediation von erkannten High-Risk-Findings
- Bewertung des Remediation Plans
- Ausstellung Zertifikat


Zertifikat

Eine **Zertifizierung** ist nur einschließlich der **Überwachung** möglich

Ablauf und Aufrechterhaltung der ZT DS Zertifizierung

ZIVILTECHNIKER OLIVER PÖNISCH

Scope
- Prüfweite / -tiefe / -umfang
- Zielsetzung und Hintergrund
- ggf. Priorisierung
- Erstellung des Auditprogrammes


Auditauftrag


Auditprogramm

Delta-Begutachtung
- Schaffung eines Gesamt(System)Überblicks
- Sicherstellung primärer Anforderungen
- Proof-of-Concept / -Design ggf. mit Stichproben
- Erstellung eines *Compliance-Risk-Reports (CRR)*
- Erstellung des Basis-Gutachtens zur Zertifizierung


Auditplan


CRR


Δ Gutachten

Zertifizierung (Überwachung)
- ggf. Überprüfung Remediation von erkannten High-Risk-Findings
- Bewertung des Remediation Plans
- Ausstellung Zertifikat


Zertifikat

Eine **Zertifizierung** ist nur einschließlich der **Überwachung** möglich

ZT DS Zertifizierung Prüfung

ZIVILTECHNIKER OLIVER PÖNISCH

- Thema Organisation/Prozesse
  - Dokumentation
  - Datenschutzorganisation
    - Datenschutzmanagement (Stichwort: DSB)
    - Data Privacy-by-Design / -Default
    - Mitarbeiter Sensibilisierung
  - Datenschutz Management Prozessen
    - Management von Verarbeitungstätigkeiten
    - Management von Datenschutzzwischenfällen
    - Datenschutzfolgeabschätzung
    - Abwicklung von Betroffenenrechten
  - (Technisch) Organisatorische Maßnahmen
    - Informationssicherheit
    - Sonstige (Pseudonymisierung)
    - Löschkonzepte

ZT DS Zertifizierung Prüfung

ZIVILTECHNIKER OLIVER PÖNISCH

- Thema Technik
  - Überprüfung der Löschung
  - Cookies
  - IT-Sicherheit
  - Technisch (Organisatorische) Maßnahmen
- Thema Recht

Ziviltechniker Oliver Pönisch

Ziviltechniker für das Fachgebiet Informationstechnologie und Telekommunikation

International zertifizierter Datenschutzexperte
CIPP / E | CIPM | CIPT

oliver.poenisch@ztop.at
+43 676 55 46 748

Kompetent . Lösungsorientiert . Staatlich befugt

Ich bin seit 20 Jahren in unterschiedlichen Rollen im Bereich der IT tätig und widme mich seit mehr als 12 Jahren der vollen Breite des Datenschutzes, der Datensicherheit und generellen IT-Compliance. Mich hat meine Leidenschaft für dieses Thema einmal quer über den Globus gebracht, und Zugang zu den heiligen Hallen der Schwerindustrie bis hin zu Feldzelten von NGOs gewährt.

Mein Anspruch war stets jene Dinge zu verfolgen, die großen Einfluss auf unsere Gesellschaft in ihrem Tun und Handeln haben und meinen Teil zu deren Weiterentwicklung zu leisten.

Ich möchte Sie herzlich einladen, sich mit meinen Leistungen vertraut zu machen und freue mich bald von Ihnen zu hören.