ITKwebcollege.DATENSCHUTZ

DIN EN ISO/IEC 17024 zertifizierter DSB

Inhalte

Teil 01 Qualifikation des Datenschutzbeauftragten nach DIN EN ISO/IEC 17024

- ✓ Erläuterungen zur DIN EN ISO/IEC 17024 als Norm zur Personenzertifizierung
- ✓ Die Zertifizierungsstelle GLOBAL-CERT

Anforderungen an den Datenschutzbeauftragten nach DIN EN ISO/IEC 17024

- ✓ Anforderung an den zertifizierten Datenschutzbeauftragten
- ✓ Mindestanforderungen gem. Vorgaben des Düsseldorfer Kreises
- ✓ Qualifikation des Datenschutzbeauftragten nach DIN EN ISO/IEC 17024
- ✓ Benötigte Unterlagen, Nachweise und Dokumente

Prüfung nach DIN EN ISO/IEC 17024

- ✓ Zertifizierung und Prüfung
- ✓ Facharbeit
- ✓ Anforderungen an die Offenen Fragen und Multiple Choise
- ✓ Bewertung und Verweis auf Prüfungsordnung

Zertifizierung

- ✓ Erhalt der Fachkunde (Qualifikationsnachweis)
- ✓ Re-Zertifizierung nach 3 Jahren

Teil 02 Datenschutzbeauftragter nach DIN EN ISO/IEC 17024

- ✓ Die Stellung, Verpflichtung, Ausbildung des Datenschutzbeauftragten
- ✓ Die Aufgaben des Datenschutzbeauftragten
- ✓ Anforderungen an einen Datenschutzbeauftragten
- ✓ Die Rechte des Datenschutzbeauftragten
- ✓ Pflichten des Datenschutzbeauftragten

Tätigkeiten des DSB

- ✓ Vorabkontrolle
- ✓ Datenschutzaudit - generelle Aufgaben und Vorgehen
- ✓ Verfahrensverzeichnis nach BDSG
- ✓ Datenträgermanagement
- ✓ Prüfung von physikalischen Absicherungen

Teil 03 Datenschutz Grundlagen

- ✓ Unterscheidung Datenschutz -Datensicherheit
- ✓ Landesdatenschutzgesetze
- ✓ Bundesdatenschutzgesetz
- ✓ Betroffenenrechte
- ✓ 7 Säulen des Datenschutzes
- ✓ Der Düsseldorfer Kreis

Das Bundesdatenschutzgesetz

- ✓ Aufbau des Gesetzes (6 Abschnitte)
- ✓ Begriffsbestimmungen
- ✓ Neuerungen im BDSG
- ✓ Kündigungsschutz des DSB
- ✓ Haftung gem. BDSG
- ✓ §42a BDSG Selbstanzeige bei Datenverlust
- ✓ Regelung der Auftragsdatenverarbeitung

Teil 04 Technisch, organisatorische Maßnahmen

- ✓ Was verlangt der Gesetzgeber von mir
- ✓ Zutrittskontrolle
- ✓ Zugangskontrolle
- ✓ Zugriffskontrolle
- ✓ Weitergabekontrolle
- ✓ Eingabekontrolle
- ✓ Auftragskontrolle
- ✓ Verfügbarkeitskontrolle
- ✓ Trennungsgebot

Organisatorische Maßnahmen, rechtliche Grundlagen

- ✓ Strafrecht / Zivilrecht im Datenschutz

Prüfungsziele von IT-Systemen

- ✓ Datensicherungssysteme
- ✓ Firewall Systeme
- ✓ Mobile Endgeräte
- ✓ Sicherheitsbereiche
- ✓ Videoüberwachung
- ✓ Technische Rechteverwaltung
- ✓ Papierdaten (Schredder)

Teil 05 § 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

- ✓ Abgrenzung ADV von Funktionsübertragung
- ✓ Wann ist eine Verarbeitung ADV
- ✓ Inhalte der Vertraglichen Regelung
- ✓ Prüfung der technisch organisatorischen Maßnahmen
- ✓ Kontrollpflicht
- ✓ IT-Wartungsfirmen BDSG §11 Abs. 5

Teil 06 Europäischer Datenschutz

- ✓ Sitzlandprinzip
- ✓ Datenübermittlung in der EU
- ✓ Europäischer Datenschutzbeauftragter
- ✓ Artikel 29- Datenschutzgruppe
- ✓ Datenschutz in den EU Ländern

EU Datenschutz Grundverordnung

- ✓ Unterscheidung EU Richtlinie – deutsches Gesetz
- ✓ Aktueller Stand
- ✓ Wichtigste Elemente der EU-DS-GVO
- ✓ Auswirkungen für den DSB
- ✓ Datenschutz Verstöße und Haftungsrisiken

Teil 07 Drittländer Datenübermittlung Rechtsgrundlagen

- ✓ Vertragserfüllung
- ✓ Einwilligung
- ✓ Gesetzlicher Ausnahmetatbestand
- ✓ Angemessenes Datenschutzniveau
- ✓ Individueller Datenschutzvertrag
- ✓ EU-Standardvertragsklauseln
- ✓ Bindig Corporate Rules
- ✓ Safe Harbor
- ✓ Betriebsvereinbarung

EU Standardvertragsklauseln

- ✓ Varianten
- ✓ Gültigkeit
- ✓ Auftragskontrolle im Ausland

Teil 08 Drittländer -USA - Safe Harbor –Principles

- ✓ 1. Informationspflicht: die Unternehmen müssen die Betroffenen darüber unterrichten, welche Daten sie für welche Zwecke erheben und welche Rechte die Betroffenen haben.
- ✓ 2. Wahlmöglichkeit: die Unternehmen müssen den Betroffenen die Möglichkeit geben, der Weitergabe ihrer Daten an Dritte oder der Nutzung für andere Zwecke zu widersprechen.
- ✓ 3. Weitergabe: wenn ein Unternehmen Daten an Dritte weitergibt, muss es die Betroffenen darüber und die unter 2. aufgeführte Wahlmöglichkeit informieren.
- ✓ 4. Zugangsrecht: die Betroffenen müssen die Möglichkeit haben, die über sie gespeicherten Daten einzusehen und sie ggfs. berichtigen, ergänzen oder löschen können.
- ✓ 5. Sicherheit: die Unternehmen müssen angemessene Sicherheitsvorkehrungen treffen, um die Daten vor unbefugtem Zugang oder vor Zerstörung und Missbrauch zu schützen.
- ✓ 6. Datenintegrität: die Unternehmen müssen sicherstellen, dass die von ihnen erhobenen Daten korrekt, vollständig und zweckdienlich sind.
- ✓ 7. Durchsetzung: die dem Safe Harbor beigetretenen Unternehmen verpflichten sich zudem, Streitschlichtungsmechanismen beizutreten, so dass die Betroffenen ihre Beschwerden und Klagen untersuchen lassen können und ihnen im gegebenen Fall Schadensersatz zukommt.

Sicht der EU / der deutschen Aufsichtsbehörden zu Safe Harbor

- ✓ Anforderungen des Düsseldorfer Kreises
- ✓ Sicht der EU

Teil 09 Standards in der Datenvernichtung

- ✓ Physische Vernichtung - Vernichten nach der aktuellen DIN-Norm 66399
- ✓ Sicherheitsklassen bei physischer Vernichtung
- ✓ Unterkategorien für Medien

Bring Your Own Device (BYOD)

- ✓ Technische Voraussetzungen für eine datenschutzkonforme Umsetzung
- ✓ Technisch-organisatorische Maßnahmen
- ✓ Risiken und Nutzen

Konzernstrukturen und Datenschutz

- ✓ Konzern – Definition
- ✓ Konzern – Aufgaben im Datenschutz
- ✓ Organisationsformen (Einheitsmodell und Koordinationsmodell)
- ✓ Privacy Code of Conduct (Binding Corporate Rules)
- ✓ Fachkonzept Datenschutz

Teil 10 Die Norm DIN EN ISO/IEC 17024

- ✓ Datenschutzbeauftragter nach DIN EN ISO/IEC 17024
- ✓ Anforderungen an einen Datenschutzbeauftragten

Zertifizierungsprüfung

- ✓ Zeichensatzung / Logoverwendung
- ✓ Online-Prüfung
- ✓ Facharbeit
- ✓ Fachgespräch
- ✓ Bewertung der Ergebnisse
- ✓ Notwendige Prüfungsunterlagen
- ✓ Allgemeine Zulassungsvoraussetzungen
- ✓ Termine

Qualifikation des Datenschutzbeauftragten nach DIN EN ISO/IEC 17024

- ✓ Erstzertifizierung
- ✓ Überwachung
- ✓ Re-Zertifizierung