

Zertifikat für Datenschutz und Informationssicherheit

Integrierter Ansatz auf Basis ISO 27001 und ISO 27701



MOTIVATION UND NUTZEN

Die Norm ISO 27701:2019 dient zum Nachweis der Einhaltung datenschutzrechtlicher Vorschriften und stellt eine Erweiterung der bekannten ISO 27001 dar. Sie ergänzt den Standard für Informationssicherheitsmanagementsysteme (ISMS) um eine Reihe wesentlicher Datenschutzaspekte.

Der offizielle Titel der Norm: „ISO/IEC 27701:2019-08 – Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden“.

Nicht nur der Titel zeigt die thematische Zusammengehörigkeit innerhalb der ISO 27000 Normenfamilie und wie stark Informationssicherheit und Datenschutz miteinander verbunden sind. Beide Normen und das gemeinsame Managementsystem basieren auf den Prinzipien Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen. So ist das Zusammenwirken dieser ISO Normen wenig überraschend und eine gemeinsame Implementierung ist sehr empfehlenswert.

Zusätzlich zum ISMS in ISO 27001 gibt die ISO 27701 eine konkrete Anleitung für die Implementierung eines Privacy Information Managementsystems (PIMS) – einem speziell um Datenschutzaspekte erweiterten integralen Teil des bestehenden ISMS. Das PIMS gibt Ihnen mehr Kontrolle über personenbezogene Daten, bietet Ihnen die Möglichkeit, Ihre personenbezogenen Daten zu verwalten und sie mit anderen Anwendern zu teilen, wenn Sie es wünschen.

Mit dem Managementsystem nach ISO 27701 erfolgt eine systematische Weiterentwicklung der Organisation inklusive der Prozessoptimierung im Bereich des Datenschutzes. Interne und externe Audits sollen dabei unterstützen.

Die Vorteile einer Zertifizierung für Organisationen liegen demnach auf der Hand:

- Sie bietet ein systemisch klares Steuerungsinstrument und Kontrollsystem für alle Datenschutzthemen, die es zu bewältigen gilt, sowie für den Umgang mit schützenswerten und personenbezogenen Daten.
- Nachweis eines DSGVO konformen Umgangs und einer datenschutzrechtlich unbedenklichen Verarbeitung sensibler Daten.
- Das risikobasierte Vorgehen kann etwaige Haftungsfelder frühzeitig aufspüren und verhindern.

- Durch den integrierten Ansatz eines PIMS für Informationssicherheit und Privacy bietet sich eine Reihe von Vorteilen integrierter Managementsysteme, so z. B. eine rasche Implementierung, ein gemeinsames Risikomanagement und eine deutliche Effizienzsteigerung durch zahlreiche Synergieeffekte.

CIS bietet als einer der ersten international akkreditierten Anbieter das Zertifikat für Datenschutzmanagement nach ISO 27701 – als Add-On zu ISO 27001 – welches einen objektiven Nachweis für DSGVO orientierten Datenschutz in Ihrem Unternehmen darstellt. Das Zertifikat schafft Vertrauen – nach innen wie auch nach außen – und ist ein klares Signal am Markt.

ZIELE

- Erhöhung der Rechtssicherheit und Transparenz
- Sicherstellung solider Datenschutzmechanismen
- Erhöhung der Datenschutzkompetenz
- Risikominimierung für Datenschutzverletzungen und Konsequenzen daraus
- Vertrauensbildung bei bestehenden und potenziellen Kunden



ZIELGRUPPE

Dieser generisch aufgebaute Standard richtet sich an alle Arten und Größen von Organisationen mit Anforderungen an einen umfassenden Schutz von Daten und Informationen – unabhängig von Branche und Gesellschaftsform.

ANFORDERUNGEN

Voraussetzung für eine erfolgreiche Zertifizierung nach ISO 27701 ist ein gültiges ISO 27001 Zertifikat. Aufgrund der inhaltlichen Nähe zur Informationssicherheit kann bei der neuen Datenschutzerklärung auf vorhandene Systeme und Strukturen aufgebaut werden. Das bedeutet in vielen Fällen nur geringen Mehraufwand für betroffene Unternehmen. Insbesondere für bereits DSGVO konform arbeitende Organisationen ist davon auszugehen, dass große Teile der Anforderungen und Maßnahmen ohnehin bereits umgesetzt sind, da die ISO 27701 weitgehend an die Regelungen der DSGVO anknüpft.

ANDERE RELEVANTE NORMEN

- ISO/IEC 27001 bzw. ISO/IEC 27002
- ISO/IEC 27018
- ISO/IEC 29100 und ISO/IEC 29151
- DSGVO

CIS STELLT SICH VOR

Als akkreditierter Zertifizierungspartner ist CIS auf Informationssicherheit, Datenschutz, IT-Services, Cloud Computing, Rechenzentren sowie auf Business Continuity Management spezialisiert. Das international hohe Ansehen von CIS-Zertifikaten erweist sich oftmals als deutlicher Vorteil im Wettbewerb – sowie auch als „Türöffner“ in weltweiten Genehmigungsverfahren. Grund dafür ist die staatliche Akkreditierung durch das österreichische Wirtschaftsministerium. Darüber hinaus kann der erprobte Zertifizierungsablauf einen erheblichen Mehrwert für die Organisationen generieren. Im Rahmen eines Zertifizierungsprojekts bringen CIS-Auditoren ihr profundes Fachwissen in der Vorbereitungsphase und in den Audits aktiv ein.



Klaus Veselko

Prokurist
CIS - Certification & Information Security Services GmbH

klaus.veselko@cis-cert.com



CIS
Certification & Information
Security Services GmbH

www.cis-cert.com



office@cis-cert.com
Salztorgasse 2/6/14,
1010 Wien, Austria
Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89