TÜVNORD

Inspired by Knowledge

Die ISO 27701 als Ergänzung zur ISO 27001

Schutz personenbezogener Daten

Die moderne Wirtschaft ist datengetrieben. Damit gewinnt der Schutz sensibler Informationen immer mehr an Bedeutung für Unternehmen. Mit einem effizienten Datenschutzmanagementsystem und einer Zertifizierung nach ISO 27701 weisen Sie nach, dass Sie beim Umgang mit personenbezogenen Daten hohe Sicherheitsstandards befolgen. Sie erfüllen leichter gesetzliche Anforderungen, beugen folgenschweren Verstößen vor und fördern das Vertrauen von Kund:innen und Mitarbeitenden.

Die ISO/IEC 27701 ist eine Erweiterung der ISO/IEC 27001. Sie enthält Leitlinien für einen sorgfältigen Umgang mit personenbezogenen Daten in Unternehmen. Unter anderem definiert sie die Rollen Controller (PII-Verantwortlicher) und Prozessor (PII-Auftragsverarbeiter).

Voraussetzung für eine Zertifizierung ist, dass Unternehmen ein Datenschutzmanagementsystem einführen, welches die Anforderungen des Standards erfüllt. Außerdem ist eine Zertifizierung nur in Verbindung mit einem Informationssicherheitsmanagementsystem nach ISO 27001 möglich. Dabei überprüfen wir Ihr Datenschutzmanagementsystem in zwei Audits, von denen eines in jedem Fall vor Ort stattfindet.

Zielgruppen für die Zertifizierung
Grundsätzlich eignet sich eine ISO 27701 Zertifizierung für jede Organisation, die personenbezogene Daten verarbeitet, unabhängig von ihrer Größe und Art. Besonders gilt das für Organisationen, die

- das Risiko von Datenschutzverletzungen und ihrer Konsequenzen (zum Beispiel hohen Geldbußen und Imageschäden) minimieren möchten,
- einen risikobasierten Ansatz für die Aufbewahrung und Verarbeitung personenbezogener Daten verfolgen müssen,
- ein ISMS betreiben und sich als Controller und/oder Prozessor weiterentwickeln möchten.

Vorteile der Zertifizierung
Mit einer Zertifizierung nach ISO 27701 profitieren Sie von folgenden Vorteilen:

- **Verringerung von Datenschutzrisiken:** Durch ein systematisches Datenschutzmanagementsystem nach ISO 27701 optimieren Sie den Schutz personenbezogener Daten und verringern das Risiko von Datenlecks.
- **Nachweis der Einhaltung von Datenschutzgesetzen:** Mit einer ISO 27701 Zertifizierung weisen Sie nach, dass Sie geeignete organisatorische und technische Maßnahmen ergriffen haben, um die Anforderungen des Bundesdatenschutzgesetzes (BDSG) zu gewährleisten.
- **Wettbewerbsvorteile:** Sie belegen Kund:innen und Geschäftspartner:innen gegenüber, dass Ihr Unternehmen im Datenschutz hohe Anforderungen erfüllt. Das wirkt sich positiv auf das Image Ihres Unternehmens aus und sorgt für Wettbewerbsvorteile.
- **Weniger Aufwand für Compliance-Projekte:** Aufgrund der systematischen Arbeit am Datenschutz und der strukturellen Prüfung durch den Zertifizierungsprozess behalten Sie den Überblick über den Status quo im Bereich Datenschutz in Ihrem Unternehmen und die aktuelle Gesetzgebung bei Compliance-Projekten. Oftmals verringern Unternehmen durch eine ISO 27001- und ISO 27701 Zertifizierung sogar den Aufwand im Rahmen von Lieferantenbewertungen.

Wichtig: Durch ein Datenschutzmanagementsystem nach ISO 27701 erfüllen Unternehmen nicht automatisch die Anforderungen der DSGVO. Sie können diese aber in das Managementsystem integrieren. Außerdem lassen sich durch den Nachweis einer ISO 27701 Zertifizierung DSGVO-Strafen oftmals verringern oder sogar vermeiden.

Voraussetzung für eine Zertifizierung
Voraussetzung für eine ISO 27701 Zertifizierung ist, dass Ihr Unternehmen ein Informationssicherheitsmanagementsystem (ISMS) besitzt, das entweder

- bereits nach ISO 27001 zertifiziert ist oder
- in Begriff ist, eine ISO 27001 Zertifizierung zu erlangen, und dass diese im Vorfeld mit positiven Auditergebnissen abgeschlossen wurde.

Die ISO 27701 ist also eine Erweiterung der Anforderungen und Kontrollen der ISO 27001 und funktioniert nicht stand-alone. Sie hat daher zwingend denselben Scope wie das basierende ISO 27001 Managementsystem.

Voraussetzung zur ISO 27701 Zertifizierung:
Das Unternehmen ist bereits nach ISO 27001 zertifiziert oder aber - mit im Vorfeld positiven Auditergebnissen - im Begriff, eine ISO 27001 Zertifizierung zu erlangen.

Ihr Weg zur ISO 27701 Zertifizierung in 7 Schritten

1. Anfrage, Angebotserstellung & -erläuterung
2. Beauftragung & individuelle Terminplanung
3. Audit: Verstehen der Organisation & Feststellung der Zertifizierungsreife
4. Aufzeigen von Verbesserungspotenzialen
5. Schnelle Vier-Augen-Prüfung & Zertifikatserstellung
6. Außenwirksames TÜV-Zertifikat
7. Kontinuierliche Weiterentwicklung des Managementsystems & der Wettbewerbsfähigkeit

Unser Know-how für Ihren Erfolg
TÜV NORD CERT ist ein international anerkannter und zuverlässiger Partner für Prüf- und Zertifizierungsdienstleistungen. Unsere Sachverständigen und Auditoren verfügen über fundiertes Wissen und haben grundsätzlich eine Festanstellung bei TÜV NORD. Hierdurch sind Unabhängigkeit und Neutralität sowie Kontinuität bei der Betreuung unserer Kunden gewährleistet. Der Vorteil für Sie liegt auf der Hand: Unsere Auditoren begleiten und unterstützen die Entwicklung Ihres Unternehmens und geben Ihnen ein objektives Feedback.

Kontakt

TÜV NORD CERT
Am TÜV 1
45307 Essen

T 0800 245-7457
F 0511 9986 69-1900

tuev-nord-cert.de

Weitere Informationen und Kontaktformular:

24-0570-10/23