ISO 27701
Datenschutz-Managementsystem

WHITEPAPER
ISO 27701

Die Norm ISO 27701 befasst sich mit der Entwicklung, Implementierung, Pflege und kontinuierlichen Verbesserung des Datenschutz-Informationsmanagementsystems (engl. „Privacy Information Management System“, kurz PIMS). Sie stellt eine Erweiterung zu dem bereits etablierten Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 und den Anforderungen des Verhaltenskodex für Informationssicherheitskontrollen gemäß ISO/IEC 27002 dar.

In der Norm wurden die Anforderungen verschiedener nationaler Gesetze, wie z.B. des GDPR, sowie die Datenschutzprinzipien der ISO/IEC 29100 vereint. Das macht die ISO 27701 zum international vorherrschenden Standard für den Umgang mit Datenschutzrisiken und dem Schutz personenbezogener Daten.

Datenschutz definieren

Während der Datenschutz die Daten vor unberechtigtem Zugriff schützt, befasst sich die Sicherung von Daten und Privatsphäre damit, welche Personen die Berechtigung für relevante Zugänge erhalten und wie diese Zugangsberechtigung im Unternehmen definiert wird. Personenbezogene Informationen (engl. „Personally Identifiable Information“, kurz PII) wie Namen, Sozialversicherungsnummern, Adressen, Telefonnummern und weitere ähnliche Informationen können einer Person direkt zugeordnet werden und haben so das Potential, die Identität einer Person aufzudecken. Aus diesem Grund müssen diese sensiblen Daten während der Erfassung, Verwendung und Weitergabe besonders geschützt werden.

Mit 4,13Milliarden Internet-Nutzern weltweit (Stand 2019)[1] und 7.098 Datenverletzungen, die im Jahr 2019 mehr als 15,1 Milliarden Datensätze enthüllt haben, wächst die globale Besorgnis hinsichtlich des Datenschutzes[2].

Eine Befragung aus dem Jahr 2019 zeigt, dass sich acht von zehn Personen (78%) Sorgen um den Schutz ihrer Privatsphäre im Internet machen. Im Gegensatz zum Vorjahr, haben sich diese Sorgen bei mehr als der Hälfte (53%) der Befragten, sogar noch verstärkt. Dieser Trend zeigte sich bereits das fünfte Jahr in Folge[3].

1 https://de.statista.com/statistik/daten/studie/805920/umfrage/anzahl-der-internetnutzer-weltweit/
2 https://www.riskbasedsecurity.com/2020/02/10/number-of-records-exposed-in-2019-hits-15-1-billion/
3 https://www.cigionline.org/internet-survey-2019

Die Relevanz der ISO 27701

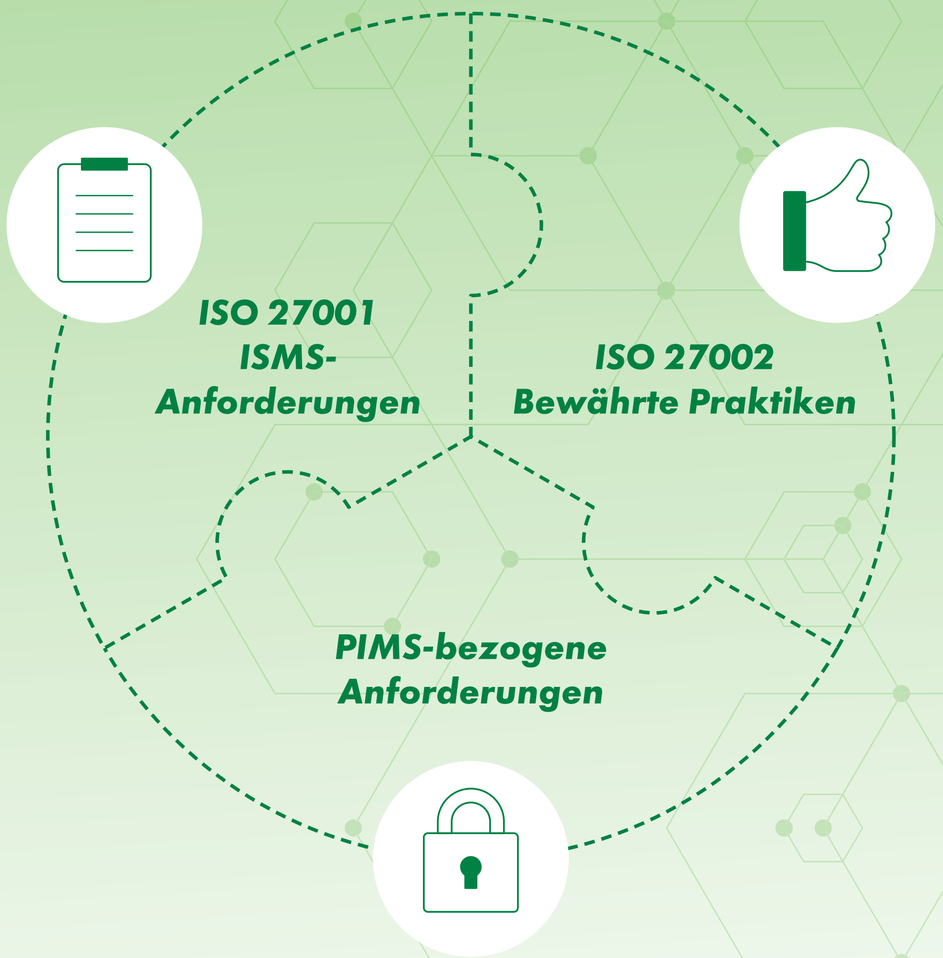
Fast jede Organisation verarbeitet personenbezogene Informationen (PII), einschließlich Privat-, Kunden- und Mitarbeiterdaten. Wenn Organisationen wachsen, expandieren oder neue Technologien verwenden, steigen sowohl der Umfang als auch die Vielfalt der durch das Unternehmen verarbeiteten PII. Geltende Datenschutzgesetze und -vorschriften müssen daher weltweit den sich verändernden Anforderungen und Risiken der Online-Umgebung angepasst werden. Die im Sommer 2019 veröffentlichte ISO 27701 ist die aktuelle Standarderweiterung zur bekannten Norm ISO 27001, welche die Anforderungen an ein effektives Informationssicherheitsmanagementsystem (ISMS) festlegt. Im Rahmen der neuen Norm ISO 27701 wurden Komponenten zur Unterstützung eines wirksamen Datenschutz- und Informationsmanagementsystem (PIMS) hinzugefügt. Dadurch bietet sie Leitlinien zur Erweiterung eines bereits existierenden ISMS. Die ISO 27701-Zertifizierung wird ausschließlich als Ergänzung zur ISMS-Zertifizierung nach ISO/IEC 27001 erteilt.

Die Vorteile der ISO 27701

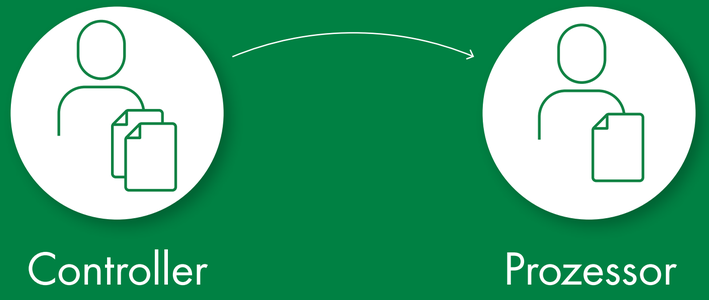
- Zuverlässige Unterstützung von Controllern und Verarbeitern hinsichtlich Datenschutzgesetzen und -vorschriften
- Erfüllung der Anforderungen von Standards wie GDPR, UK DPA, HIPPA und CCPA sowie anderen ISO-Normen
- Praktikable, klare Maßnahmen zum Schutz von PII
- Gesteigertes Bewusstsein für Vertrauen und Datenschutz
- Sicherstellung der Transparenz zwischen den Interessengruppen

Die drei Komponenten der

ISO 27701 Zertifizierung



Rollen und *Datenschutz-Management*



Herausforderungen bei der Einhaltung der Vorschriften

Die ISO 27701 befasst sich mit drei zentralen Herausforderungen bei der Einhaltung von Vorschriften:

- **Vielzahl regulatorischer Anforderungen**
  Durch den Einsatz einer Reihe von allgemeingültigen Kontrollelementen, können die verschiedenen regulatorischen Anforderungen in Einklang gebracht werden. Dadurch wird eine konsistente und effiziente Umsetzung ermöglicht.

- **Kostenintensive Prüfung der einzelnen Vorschriften**
  Sowohl interne als auch externe Prüfer können die Einhaltung der Vorschriften unter Verwendung eines universellen Kontrollsystems innerhalb eines einzigen Prüfungszyklus beurteilen.

- **Risiko der Nichtkonformität ohne Nachweis**
  Handelsvereinbarungen, die die Weitergabe von persönlichen Informationen beinhalten, können eine Zertifizierung der Konformität rechtfertigen[4].

Definierte Rollen im Datenschutz-Management

Die in der Norm ISO 27701 festgeschriebenen Rollen sind Controller und Prozessor. Diese Rollen werden in Artikel 4 der GDPR oder in der Norm ISO 29100 definiert.

- Ein **Controller** ist eine „natürliche oder juristische Person, Behörde, Agentur oder eine andere Stelle, die allein oder gemeinsam mit anderen, die Intentionen und Mittel der Verarbeitung von persönlichen Daten bestimmt".

4 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3uDwE

- Ein **Prozessor** ist eine „natürliche oder juristische Person, Behörde, Agentur oder andere Stelle, die personenbezogene Daten im Namen des Controllers verarbeitet“[5].

Die Struktur der ISO 27701

Die Norm ISO 27701 ist in datenschutzzentrierte Klauseln (5-8) und Anhänge (A-F) untergliedert.

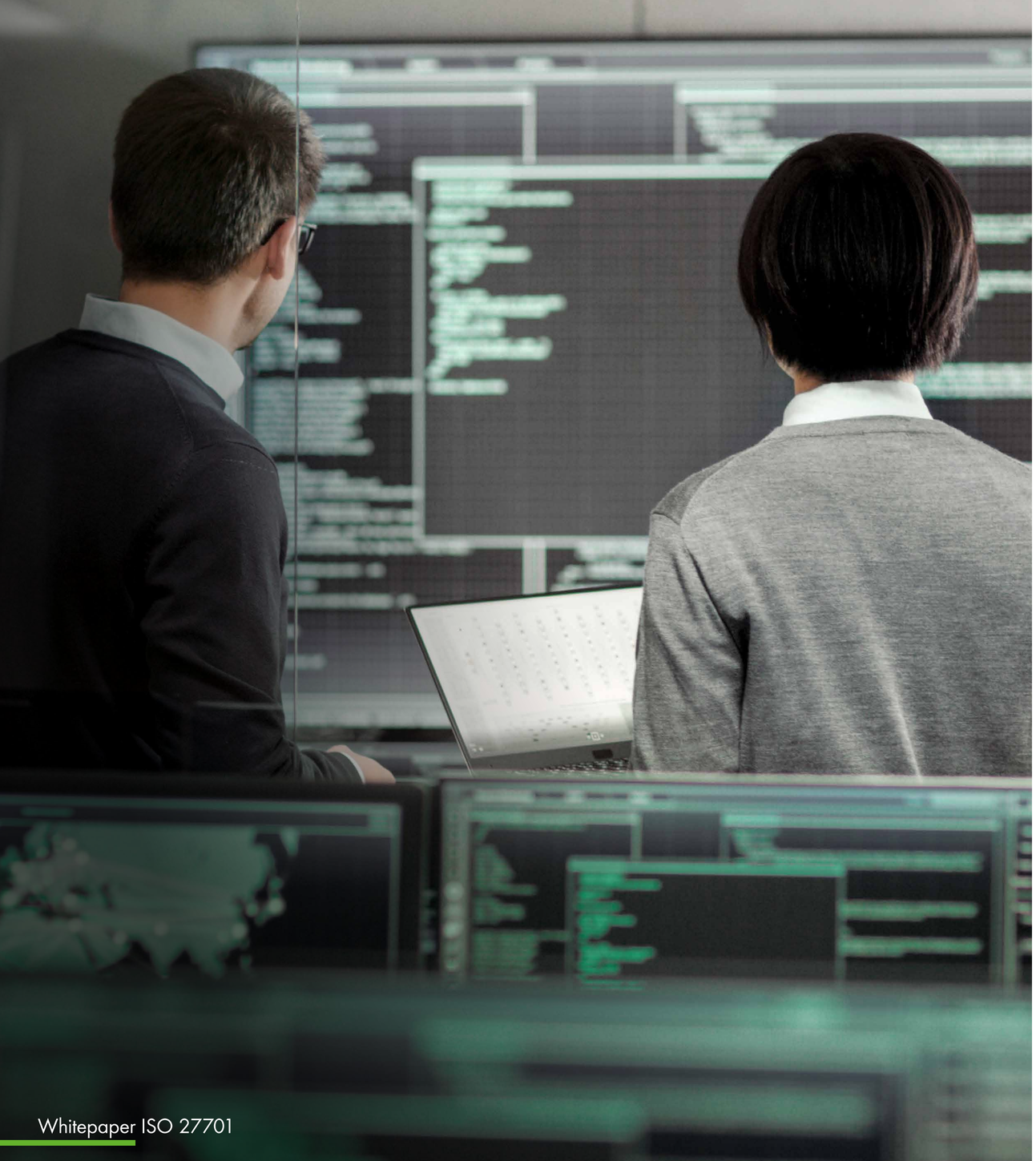
Die Klauseln enthalten zusätzliche Anforderungen oder Implementierungsanleitung einschließlich:

- PIMS-spezifische Änderungen an der ISO 27001 (Abschnitt 5)
- PIMS-spezifische Anforderungen an die ISO 27002 (Abschnitt 6)
- Zusätzliche Anforderungen zur ISO 27002 für PII Controller (Paragraf 7)
- Zusätzliche Anforderungen zur ISO 27002 für PII Prozessor (Paragraf 8)

Sechs relevante Anhänge bieten Orientierungshilfen für Standardthemen wie:

- PII Prozessor (Anhang B)
- Abbildung nach ISO 29100 (Anhang C)
- Mapping zu GDPR (Anhang D)
- Abbildung nach ISO 27018 & 29151 (Anhang E)
- Mapping nach ISO 27001 & 27002 (Anhang F)

5 https://ec.europa.eu/info/law/law-topic/data-protection_en



Die Integration der ISO 27701 in verschiedene ISMS-Setups

Die ISMS-Erweiterung nach ISO 27701 ist für Organisationen, die bereits ISO/IEC 27017 oder ISO/IEC 27018 in ihr bestehendes Managementsystem integriert haben, eine größere Herausforderung. Es müssen wesentliche Änderungen an der ISMS-Gesamtstruktur, an den bestehenden in Anhang A beschriebenen Controls und an der Umsetzung der Kontrollziele vorgenommen werden, die für PII-Prozessor und -Controller relevant sind.

Der Übergang zur ISO 27701 kann dagegen für Organisationen, deren Strukturen und Prozesse, die GDPR-Anforderungen unterstützen, etwas einfacher sein.

In beiden Fällen muss jedoch die angemessene und effektive Implementierung der Prozesse in den Geltungsbereich des ISMS gewährleistet sein.
Die erfolgreiche Implementierung der ISO 27701 in ein bestehendes Informationssicherheitsmanagementsystem (ISMS) ist abhängig von der:

- GAP Analyse des bestehenden ISMS gemäß der Anforderungen nach ISO 27701
- Identifizierung von Lücken sowie der Erstellung eines Maßnahmenplans zur Behebung dieser
- Anpassung des Geltungsbereichs
- Anpassung der Controls der ISO 27001 an die neuen Anforderungen
- Aufklärung, ob Sie ein PII Controller, -Prozessor oder höchstwahrscheinlich beides sind

- Erweiterung der Anwendbarkeitserklärung (Statement of Applicability, SOA) oder Erstellung einer neuen SOA für Anhang A und B von ISO 27701
- Liste der Verarbeitungsvorgänge
- Erweiterung der Vermögensverwaltung
- Aufnahme neuer Anforderungen in das ISMS-Konzept
- Bewertung des erweiterten ISMS mit Hilfe von Risikobewertung, Messungen und Überwachung, interner Revision, Managementprüfung und anderen relevanten Bewertungsinstrumenten

Um sicherzustellen, dass das erweiterte ISMS sowohl die bereits bestehenden als auch die neuen Anforderungen erfüllt, werden die betrieblichen Leistungen gemessen. Für Bereiche, die in jeglicher Hinsicht mangelbehaftet oder nicht konform zur ISO 27701 sind, müssen kontinuierliche Verbesserungsstrategien oder Korrekturmaßnahmen festgelegt werden.

Ordnungsgemäße Aufzeichnung von Verstößen

Alle Verstöße gegen die PII müssen festgehalten werden, um einen Bericht für behördliche und/oder forensische Zwecke zu erstellen. Dieser Bericht sollte die folgenden Punkte beinhalten:

- Beschreibung und Zeitraum des Vorfalls
- Folgen des Vorfalls
- Name der Person, die den Vorfall gemeldet hat
- Name der Person, der dieser Vorfall gemeldet wurde

- Schritte die zur Lösung des Vorfalls unternommen wurden (einschließlich der verantwortlichen Person und der wiederhergestellten Daten)
- Beurteilung der Frage, ob der Vorfall zu Nichtverfügbarkeit, Verlust, Offenlegung oder Änderung von PII geführt hat

Support-Services zur ISO 27701

In der sich immer schneller verändernden, globalen und digitalen Wirtschaft muss sich nahezu jedes Unternehmen verstärkt mit großen Mengen elektronischer Daten befassen. Da der Schutz der Privatsphäre und die Sicherheit der Daten Hand in Hand gehen, ist der Großteil der Bemühungen für eine ISO 27701-Zertifizierung bereits unternommen, wenn Sie schon nach der ISO 27001 zertifiziert sind. Um den Schutz Ihrer personenbezogenen Daten zu gewährleisten, bieten Ihnen unsere akkreditierten Prüfer die folgende Leistungen:

- Bewertungen der Sicherheits- und Datenschutzlücken zwischen Ihrem bestehenden System und den Anforderungen der ISO 27001 und ISO 27701
- PII-Verarbeitungsbewertungen, um den Umfang der gesammelten, verarbeiteten und gemeinsam genutzten personenbezogenen Daten zu untersuchen

Benötigen Sie Unterstützung für Ihre ISO 27701-Zertifizierung? Kontaktieren Sie jetzt unsere Experten!

Weitere Leistungen, von denen Sie profitieren

Sie haben ebenfalls die Möglichkeit, weitere Zertifizierungen durch unsere erfahrenen Experten durchführen zu lassen, wie z.B. nach ISO 9001, ISO 14001, ISO 45001 und deren Kombinationen. Unser Portfolio umfasst über 40 Akkreditierungen und Zulassungen! Darüber hinaus bietet Ihnen die DEKRA Gruppe rund um das Thema Informationssicherheit:

- Aus- und Weiterbildung, z.B. zum IT-Spezialisten
- Produktzertifizierungen, z.B. elektromagnetische Verträglichkeit (EMC)
- Personenzertifizierungen, z.B. Datenschutzbeauftragter

→ Wünschen Sie weitere Informationen?

→ Kontakt

Ausgezeichnet – das DEKRA Siegel

Setzen Sie ein Ausrufezeichen für höchste Qualität und Zuverlässigkeit – branchenübergreifend und international. Das DEKRA Siegel leistet beste Dienste als Imageträger, Marketinginstrument und um sich vom Wettbewerb abzuheben. So zeigen Sie Ihren Kunden und Geschäftspartnern, dass Leistung bei Ihnen ihr Geld wert ist. Wir unterstützen Sie gerne dabei.

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra.de/audit