Bild: Adobe Stock

Das Datenschutz-Informations-Management-System kann nun als eigenständiger Standard genutzt werden, ohne dass vorher die ISO/IEC 27001 zertifiziert werden muss.

# ISO 27701:2025 – Das Datenschutz-Managementsystem

**Am 16. Oktober war es nach langer Wartezeit endlich so weit, die neue ISO 27701 wurde veröffentlicht. Nun kann das Datenschutz-Managementsystem auch ohne ein Informationssicherheits-Managementsystem nach ISO 27001 zertifiziert werden. Die Norm folgt dabei der harmonisierten Struktur (HS), ist also analog anderen Normen wie der 9001 aufgebaut.**

Wie bekannt aus anderen Normen, wird im Kapitel 1 der Anwendungsbereich definiert. Die Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Datenschutz-Informationsmanagementsystems (DSMS, englisch PIMS) fest. Der Fokus sind dabei Verantwortliche und Auftragsverarbeiter für personenbezogene Daten (PII), die für die Verarbeitung personenbezogener Daten verantwortlich und rechenschaftspflichtig sind, unabhängig von deren Art und Grösse.

**ZUM AUTOR**

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

## 25 neue Begriffe

Kapitel 2 enthält normative Referenzen, hier nur auf die ISO/IEC 29100, dem Rahmenwerk für den Datenschutz (aktuelle Ausgabe ist aus dem Jahr 2024). Im Kapitel 3 werden Begriffe, Definitionen und Abkürzungen eingeführt. Insgesamt sind es 25 neue Begriffe: Organisation, interessierte Partei, oberste Leitung, Managementsystem, Richtlinien, Ziel, Risiko, Prozess, Kompetenz, dokumentierte Information, Leistung, kontinuierliche Verbesserung, Wirksamkeit, Anforderung, Konformität, Nichtkonformität, Korrekturmassnahme, Audit, Messung, Überwachung, Gemeinsamer Verantwortlicher für personenbezogene Daten, Kunde, Datenschutz-Informationsmanagementsystem, Informationssicherheitsprogramm und Anwendbarkeitserklärung.

Das Managementsystem startet mit Kapitel 4, dem Kontext der Organisation. Dazu müssen die externen und internen Themen bestimmt werden. Die Norm erwähnt dabei geltende Datenschutzgesetze und Vorschriften, Gerichtsentscheidungen, Richtlinien und Verfahren, Verwaltungsentscheidungen oder vertragliche Anforderungen. Auch gehört der Klimawandel dazu (in den anderen Normen als Addendum ergänzt). Eine wichtige Definition ist das Feststellen, ob die Organisation als Verantwortlicher und/oder als Auftragsverarbeiter für personenbezogenen Daten fungiert.

## Den Geltungsbereich des Managementsystems festlegen

Als zweites gilt es das Verständnis für die Bedürfnisse und Erwartungen der betroffenen Parteien festzuhalten. Das können Kunden, Partner, Lieferanten oder Aufsichtsbehörden sein. Die Norm verwendet den Begriff «Kunde» (leider) für drei Arten:

- eine Organisation, die einen Vertrag mit einem PII-Verantwortlichen hat
- ein PII-Verantwortlicher, der einen Vertrag mit einem PII-Auftragsverarbeiter hat
- ein PII-Verarbeiter, der einen Vertrag mit einem Subunternehmer für die PII-Verarbeitung hat

Dies macht es nicht immer einfach festzustellen, welche Rolle genau gemeint ist. Als letzten Punkt gilt es noch den Geltungsbereich des Managementsystems festzulegen und es einzurichten, zu implementieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

Nachdem der Rahmen festgelegt ist, werden die Anforderungen an die Führung, die Norm spricht von der obersten Leitung, festgelegt. Dazu gehören die Definition der Datenschutzrichtlinien und Datenschutzzielen, das Integrieren des Datenschutzes in die Geschäftsprozesse, das Bereitstellen der erforderlichen Ressourcen, das Schaffen der Awareness, dafür zu sorgen, dass die beabsichtigten Ergebnisse erzielt, die kontinuierliche Verbesserung sowie die Unterstützung alle relevanten Funktionen sicherzustellen.

Die Norm verlangt ebenfalls, dass eine Datenschutzerklärung erstellt, dokumentiert, kommuniziert und den interessierten Parteien zur Verfügung steht. Weiter sind die Rollen, Verantwortlichen und Befugnisse festzulegen.

### Erstellen einer Anwendbarkeitserklärung

Wie in der ISO 27001 ist auch bei dieser Norm das Risiko-Management ein zentraler Punkt. Dazu muss ein Prozess zur Bewertung von Datenschutzrisiken definiert und angewendet werden. Auch müssen die Kriterien zur Bewertung der Risiken inkl. der Risiko-Akzeptanz festgelegt sein. Wichtig ist, dass wiederholte Datenschutz-Risikobewertungen konsistente, valide und vergleichbare Ergebnisse liefern. Jedes Risiko muss einem Verantwortlichen zugewiesen werden. Nicht akzeptierte Risiken gilt es entsprechend zu behandeln. Dies kann beispielsweise mit Kontrollen sichergestellt werden. Die Norm verlangt zudem ein Informationssicherheitsprogramm umzusetzen und listet dazu 15 Themen auf. Diese entsprechen den Anforderungen aus der ISO 27002. Weiter gehört das Erstellen einer Anwendbarkeitserklärung der Massnahmen aus Anhang A dazu.

Das Kapitel 6.2 verlangt die Definition von Datenschutzzielen und einen Plan zur Erreichung dieser. Sie müssen messbar sein, geltende Anforderungen berücksichtigen, überwacht, kommuniziert, aktualisiert und dokumentiert werden.

Das Kapitel 7 beschreibt die unterstützenden Themen. Dazu gehören das Bestimmen und Bereitstellen von Ressourcen, die notwendige Kompetenz festzulegen, das Bewusstsein (Awareness) der involvierten Personen sicherzustellen, die Kommunikation sowie die Dokumentation zu definieren.

Nachdem die Grundlagen geschaffen sind, wird in Kapitel 8 der Betrieb beschrieben. Es gilt die Prozesse zu planen, zu implementieren und zu kontrollieren. Damit dies möglich ist, sind die Kriterien für die Prozesse festzulegen. Änderungen sind ebenfalls zu planen. Auch müssen extern bereitgestellte Prozesse, Produkte oder Dienstleistungen kontrolliert werden.

In Kapitel 9 folgt die Leistungsbewertung. Dazu muss zuerst festgelegt werden, was überwacht und gemessen wird, die Methoden dazu sowie wann die Ergebnisse der Überwachung und Messung analysiert und bewertet werden. Ein Werkzeug dazu ist das interne Audit. Dieses muss in geplanten Abständen gemäss dem internen Audit-Programm durchgeführt werden. Das Programm definiert die Ziele, Kriterien, den Umfang sowie bestimmt objektive und unparteiische Auditoren. Die Ergebnisse sind den zuständigen Führungskräften zu melden. Der letzte Punkt legt den Rahmen für die Managementbewertung fest. Gegenüber anderen Normen sind es hier «nur» fünf Punkte.

### Noch ein 11. Kapitel

Das zweitletzte Kapitel beschreibt die Verbesserung. Die Eignung, Angemessenheit und die Wirksamkeit des Managementsystems sind kontinuierlich zu verbessern. Sollten Nichtkonformitäten festgestellt werden, ist die Ursache zu erfassen und geeignete Massnahmen zur Beseitigung umzusetzen. Im Nachgang ist die Wirksamkeit der ergriffenen Korrekturmassnahmen zu überprüfen.

Im Unterschied zu anderen Normen ist noch ein 11. Kapitel vorhanden. Es weist darauf hin, dass im Anhang C eine Zuordnung zwischen den Bestimmungen der Norm und den Datenschutzgrundsätzen aus ISO/IEC 29100, in Anhang D eine Zuordnung der Kontrollen zur Datenschutz-Grundverordnung der Europäischen Union, in Kapitel E eine Zuordnung zu den Bestimmungen aus ISO/IEC 27018 (Schutz von personenbezogenen Daten in Cloud-Diensten) und ISO/IEC 29151 (Verhaltenskodex für den Schutz personenbezogener Daten) sowie in Kapitel F ein Vergleich zur vorherigen Ausgabe der ISO 27701 aus dem Jahr 2019 abgebildet ist.

Der normative Anhang A listet im ersten Teil Kontrollziele und Kontrollen für PII-Verantwortliche auf. Sie sind unterteilt in:

- Bedingungen für die Erhebung und Verarbeitung (8 Punkte)
- Verpflichtungen gegenüber den PII-Auftraggebern (10 Punkte)
- Privacy by Design und Privacy by Default (9 Punkte)
- Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten (4 Punkte)

Der zweite Teil umfasst Kontrollziele und Kontrollen für PII-Verarbeiter. Die Kontrollen sind unterteilt in:

- Bedingungen für die Erhebung und Verarbeitung (6 Punkte)
- Verpflichtungen gegenüber den Betroffenen (1 Punkt)
- Privacy by Design und Privacy by Default (3 Punkte)
- Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten (8 Punkte)

Der dritte Teil beschreibt die Kontrollziele und Kontrollen für PII-Verantwortliche und PII-Verarbeiter. Diese wurden aus der ISO 27001, Anhang A übernommen. Die ISO 27001 umfasst 93 Massnahmen, in der ISO 27701 sind 29 davon enthalten.

### Eine Anleitung zur Umsetzung

Während die ISO 27001 in zwei Dokumente unterteilt ist, sind beide Teile in der ISO 27701 enthalten. Der Anhang B beschreibt die aus Anhang A aufgeführten Punkte, jeweils die Massnahme sowie eine Anleitung zur Umsetzung.

Gleichzeitig mit der ISO 27701 wurde auch die ISO 27706 veröffentlicht. Sie legt fest, wie akkreditierte Zertifizierungsstellen das Datenschutz-Managementsystem zu prüfen haben.

Die neue ISO/IEC 27701:2025 bringt einen deutlichen Fortschritt. Das Datenschutz-Informations-Management-System kann nun als eigenständiger Standard genutzt werden, ohne dass vorher die ISO/IEC 27001 zertifiziert werden muss. Alles in allem stellt die Revision einen ansprechenden Rahmen für Unternehmen dar, die durch Datenschutz Vertrauen aufbauen und ihre Privacy-Governance effizienter und internationaler gestalten wollen.