1/2026
1 – 24

DSB
Data Breach Geldstrafe
Haidinger/Löffler

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Cyberangriff und Verteidigung

Chronologie einer Cyberattacke
Interview Manuel Löw-Beer, risikomonitor.com

Wie Interessenverbände Tech-Konzerne angreifen
Pascal Schumacher, Lea Stegemann

Möglichkeiten des BR bei Gefährdung von AN-Daten
Monika Drs

Checkliste Cybersecurity – Verteidigung und Vorfallsbewältigung
Hans-Jürgen Pollirer

EuGH verneint die Ableitung von Unterlassungsansprüchen
Carolin Marschoun

Schutz personenbezogener Daten beim Zugang zu amtlichen Informationen
Mirjam Tercero, Jan Hospes

ISO/IEC 27701:2025 Datenschutz-Managementsysteme
Bettina Sterner

ISSN 2313-5409
dako.manz.at
MANZ

Bettina Sterner
Datenschutz- und Governance-Expertin

ISO/IEC 27701:2025 als eigenständige Norm – ein praxisnaher Rahmen für Datenschutz-Managementsysteme in KMU

Stand-Alone-Zertifizierung; Cloud; Data Breach; Risk Treatment. Mit der im Oktober 2025 in Kraft getretenen Neuerung ist ISO/IEC 27701 erstmals als eigenständige Norm zertifizierbar – ohne verpflichtende ISO/IEC-27001-Zertifizierung. Für kleine und mittlere Unternehmen (KMU) schafft dies einen praktikablen Rahmen, um Datenschutz als strukturiertes Management- und Risikothema umzusetzen. Der Beitrag erläutert die wesentlichen Neuerungen der Norm und zeigt aus Sicht von Datenschutzbeauftragten, wie ein Datenschutz-Managementsystem aufgebaut werden kann, das Entscheidungen nachvollziehbar dokumentiert und im laufenden Betrieb steuerbar bleibt.

Ausgangslage: Datenschutz zwischen Anspruch und Realität

Datenschutz ist längst kein reines Compliance-Thema mehr. Kund:innen, Geschäftspartner:innen und Aufsichtsbehörden erwarten nachvollziehbare, dokumentierte und wirksame Datenschutzprozesse. Gerade KMU stehen dabei vor einem Spannungsfeld: Einerseits wächst der regulatorische Druck, andererseits sind Ressourcen – personell wie finanziell – begrenzt.

ISO/IEC 27701 wurde 2019 als Erweiterung von ISO/IEC 27001 entwickelt, um ein **Privacy Information Management System (PIMS)** zu etablieren. In der Praxis bedeutete dies jedoch bislang, dass eine vollständige ISO/IEC-27001-Zertifizierung Voraussetzung war – ein Aufwand, der viele KMU abgeschreckt hat. Die neue Möglichkeit der **Stand-alone-Zertifizierung** ändert diese Situation grundlegend.

Was ist ISO/IEC 27701:2025 – und was regelt sie konkret?

ISO/IEC 27701 ist eine international anerkannte Norm für den Aufbau, die Umsetzung, den Betrieb und die kontinuierliche Verbesserung eines PIMS. Sie ergänzt bestehende Managementsysteme um spezifische Anforderungen an Datenschutz-Governance, Risikomanagement und Kontrolle (iSe Datenschutz-Managementansatzes). **Im Fokus stehen** insb:

- Klare Rollen und Verantwortlichkeiten im Datenschutz;
- strukturierte Prozesse für Betroffenenrechte;
- systematische Risiko- und Folgenabschätzungen;
- dokumentierte technische und organisatorische Maßnahmen;
- Steuerung von Auftragsverarbeitern und Partnern.

Für die praktische Umsetzung eines Datenschutz-Managementsystems bedeutet dies, dass diese Themen nicht isoliert, sondern als **zusammenhängende Steuerungselemente** betrachtet werden. Für Datenschutzbeauftragte (DBA) steht dabei weniger die Neuerfindung von Prozessen im Vordergrund, sondern deren strukturierte Verknüpfung, Verantwortlichkeitszuordnung und regelmäßige Überprüfung im laufenden Betrieb.

Die wesentliche Neuerung: ISO 27701 ohne ISO 27001

Seit Oktober 2025 kann ISO/IEC 27701 eigenständig zertifiziert werden, ohne verpflichtende Einführung eines vollständigen ISMS nach ISO/IEC 27001. Der Fokus liegt damit stärker auf datenschutzrelevanten Prozessen, bei zugleich geringerem Implementierungs- und Auditaufwand.

In der bisherigen Fassung war ISO/IEC 27701 konzeptionell und auditseitig eng an ISO/IEC 27001 gekoppelt, was häufig einen hohen Dokumentations- und Strukturierungsaufwand sowie einen starken Fokus auf Informationssicherheit mit sich brachte – auch dort, wo primär Datenschutzrisiken relevant waren.

Die neue Fassung stärkt ISO/IEC 27701 als eigenständigen Orientierungsrahmen für Datenschutz. Auch ohne Zertifizierungsabsicht kann die Norm genutzt werden, um bestehende DSGVO-Strukturen systematisch zu ordnen, Verantwortlichkeiten klarer zu definieren und Datenschutz messbar, überprüfbar und steuerbar zu machen. ISO/IEC 27701 ist damit weniger eine Datenschutz-Norm im klassischen Sinn als ein Rahmen für datenschutzbezogene Governance- und Risikosteuerung.

Änderungen bei Digitalisierung und Cloud

Die überarbeitete ISO/IEC 27701 trägt modernen IT-Landschaften Rechnung und adressiert Cloud-Dienste, verteilte Systeme und digitale Geschäftsmodelle explizit. **Im Fokus stehen** klarere Verantwortlichkeiten in Cloud-Konstellationen, präzisere Anforderungen an Auftragsverarbeitung und gemeinsame Verantwortlichkeit, eine bessere Anschlussfähigkeit an bestehende Cloud-Governance-Modelle sowie klarere Vorgaben zur Dokumentation technischer Maßnahmen.

Die unverkennbare DNA der ISO/IEC 27001

Auch in der neuen Stand-Alone-Fassung lässt sich die Herkunft der ISO/IEC 27701 nicht leugnen, inhaltlich und strukturell bleibt sie eng an ISO/IEC 27001 angelehnt, insb in den Annexen.

Die Kontrollziele in Annex A (PII Controller) und Annex B (PII Processor), va ab A.3 „security considerations for PII controllers and processors", entsprechen in weiten Teilen den bekannten Controls aus ISO/IEC 27001 Annex A. In der Praxis handelt es sich häufig um identische oder nur geringfügig angepasste Maßnahmen, ergänzt um den Bezug zur Verarbeitung personenbezogener Daten. **Diese Nähe ist bewusst gewählt:** ISO/IEC 27701 versteht Datenschutz nicht losgelöst, sondern als Erweiterung eines strukturierten Informationssicherheitsansatzes.

Security Incident ist nicht gleich Data Breach

Ein besonders praxisrelevanter Punkt betrifft den Umgang mit Sicherheitsvorfällen. Auch in der neuen Fassung kennt ISO/IEC 27701 **kein eigenständiges Data-Breach-**

Management iSd DSGVO. Stattdessen fordert die Norm weiterhin ein Information Security Incident Management, das – soweit relevant – auf Vorfälle iZm der Verarbeitung personenbezogener Daten angewendet wird.

Die datenschutzrechtliche Bewertung, ob ein Sicherheitsvorfall eine **Datenschutzverletzung nach Art 4 Z 12 DSGVO** darstellt und ob daraus Melde- oder Informationspflichten resultieren, wird von der Norm nicht vorgegeben. Diese Übersetzungsleistung – vom Security Incident zur Datenschutzverletzung („Data Breach") – bleibt ausdrücklich Aufgabe der Organisation und kann durch ISO/IEC 27701 nicht delegiert oder ersetzt werden. Für das Datenschutz-Managementsystem bedeutet dies, dass diese Bewertung als bewusster Entscheidungsschritt ausgestaltet und nachvollziehbar dokumentiert werden muss.

PRAXISTIPP

Incident-Management sollte als einheitlicher Governance-Prozess aufgesetzt werden, nicht als Abfolge getrennt verantworteter Einzelschritte.

Für die **Umsetzung im Datenschutz-Managementsystem** bedeutet das konkret:

- Eine zentrale Incident-Steuerung mit abgestimmten Dokumentationspunkten, bei der Sicherheitsvorfälle systematisch erfasst und einer datenschutzrechtlichen Bewertung zugeführt werden;
- ein fest definierter Entscheidungsschritt, an dem bewertet wird, ob ein Vorfall eine Datenschutzverletzung iSd DSGVO („Data Breach") darstellt;
- eine klare Zuordnung, wer diese Bewertung vornimmt bzw freigibt;
- eine dokumentierte Entscheidung, auch wenn keine Meldepflicht ausgelöst wird.

Für KMU ist es dabei nicht entscheidend, wie umfangreich diese Elemente ausgestaltet sind, sondern dass sie konsistent angewendet und nachvollziehbar dokumentiert werden.

Praxisnahe Umsetzung für KMU: Weniger ist mehr

Ein häufiger Fehler bei der Einführung von Managementsystemen ist der Versuch, „alles auf einmal" umzusetzen. Für DBA zeigt sich hier der praktische Mehrwert der ISO/IEC 27701: Gerade in der Stand-Alone-Version erlaubt sie einen modularen und risikobasierten Aufbau eines Datenschutz-Managementsystems, der sich an den tatsächlichen Datenschutzrisiken orientiert.

- **Schritt 1: Scope realistisch definieren**

Der Anwendungsbereich sollte **bewusst eng gefasst** werden: Welche Prozesse verarbeiten personenbezogene Daten? Welche Geschäftsbereiche sind besonders risikorelevant?

Aus Sicht des Datenschutz-Managementsystems dient der Scope nicht nur der Abgrenzung für eine mögliche Zertifizierung, sondern als **zentrale Steuerungsgröße:** Er legt fest, für welche Prozesse der Datenschutz systematisch geplant, überwacht und bewertet wird. Ein klar definierter Scope erleichtert es DBA, Prioritäten zu setzen und Ressourcen gezielt einzusetzen.

- **Schritt 2: Bestehende Datenschutzstrukturen nutzen**

In vielen KMU existieren bereits Verzeichnisse von Verarbeitungstätigkeiten, Datenschutzrichtlinien und Verträge zur Auftragsverarbeitung. Diese Inhalte können direkt in das Datenschutz-Managementsystem **integriert werden** – entscheidend ist nicht ihre Neuerstellung, sondern ihre Einbindung in ein einheitliches Steuerungs- und Reviewkonzept. Doppeldokumentation ist nicht erforderlich.

- **Schritt 3: Rollen pragmatisch festlegen**

ISO 27701 verlangt klare Zuständigkeiten, aber keine neuen Vollzeitrollen. In der Praxis bewähren sich eine Kombination von Datenschutz- und Compliance-Funktionen sowie klare Eskalationswege statt komplexer Gremien.

- **Schritt 4: Risiken priorisieren**

Nicht jede Verarbeitung erfordert maximale Maßnahmen. Entscheidend ist nicht allein die Risikohöhe, sondern der bewusste Umgang mit identifizierten Risiken. ISO/IEC 27701 greift hier die Logik des ISMS-Risikomanagements auf und verlangt nicht nur eine Bewertung, sondern eine nachvollziehbare Risikobehandlung **(Risk Treatment).** In der Praxis bedeutet das:

  - **Mitigation:** gezielte technische oder organisatorische Maßnahmen zur Risikominderung;
  - **Acceptance:** bewusste Risikoakzeptanz auf Managementebene, sofern verbleibende Risiken vertretbar sind;
  - **Transfer:** Verlagerung von Risiken, etwa durch vertragliche Regelungen oder organisatorische Maßnahmen;
  - **Avoidance:** bewusste Vermeidung von Risiken, etwa durch Anpassung oder Unterlassung bestimmter Verarbeitungsvorgänge.

Die Auswahl der Risikobehandlungsoption erfolgt auf Basis einer **nachvollziehbaren Risikoeinschätzung** und ist zu dokumentieren. Für die Risikobewertung können DBA dabei auf bestehende, etablierte **Risikomanagement-Ansätze aus dem Security-Bereich** (zB OCTAVE) zurückgreifen, sofern diese eine strukturierte Bewertung von Eintrittswahrscheinlichkeit, Auswirkungen und bestehenden Maßnahmen ermöglichen.

In der Risikobehandlung kann – in Anlehnung an Sicherheitskonzepte wie **ALARP („as low as reasonably practicable")** – zwischen akzeptablen Restrisiken und nicht akzeptablen Risiken differenziert werden. ALARP setzt dabei voraus, dass **Rechts- und Compliance-Risiken**, insb Gesetzesverstöße, **nicht akzeptabel sind** und daher nicht Gegenstand einer Risikoakzeptanz sein können.

Diese Einordnung unterstützt DBA in der Praxis, da ISO/IEC 27701 ein systematisches Risikomanagement für Datenschutzrisiken voraussetzt und damit die Grenze zwischen zulässiger Risikoabwägung und unzulässiger Risikoakzeptanz klar markiert. Entscheidungsprozesse gegenüber dem Management werden dadurch fachlich nachvollziehbar und belastbar abgesichert.

PRAXISTIPP

Ein dokumentiertes Risk-Treatment-Decision-Log ist für KMU und DBA oft wirkungsvoller als umfangreiche Maßnahmenkataloge, da es Entscheidungen transparent und überprüfbar macht.

Mehrwert über die Zertifizierung hinaus

ISO/IEC 27701 ist kein Selbstzweck und kein reines Compliance-Instrument. Ihr Mehrwert liegt insb darin, Datenschutz erstmals konsequent als Risikomanagement- und Steuerungsthema zu etablieren. Durch die explizite Anbindung an etablierte Risikomanagement-Logiken ermöglicht die Norm eine **strukturierte Auseinandersetzung mit Datenschutzrisiken**, die über bloße Schutzmaßnahmen hinausgeht. Organisationen sind angehalten, Risiken nicht nur zu identifizieren, sondern bewusst zu behandeln – etwa durch gezielte Minderung, begründete Akzeptanz oder Übertragung.

Gerade für KMU entsteht dadurch ein praxisnaher Orientierungsrahmen, der hilft, Datenschutzentscheidungen nachvollziehbar, konsistent und managementtauglich zu treffen. Datenschutz wird damit nicht

länger als „Alles-oder-nichts-Disziplin“ verstanden, sondern als steuerbarer Prozess, der rechtliche Anforderungen, organisatorische Realitäten und wirtschaftliche Erwägungen zusammenführt.

Auch ohne formale Zertifizierung bietet ISO/IEC 27701 damit einen strukturierten Referenzrahmen, um bestehende DSGVO-Umsetzungen zu ordnen, Prioritäten zu setzen und Entscheidungen transparent zu dokumentieren.

Übergangsregelungen und empfohlene Vorgehensweise

Für die neue ISO/IEC 27701:2025 liegen derzeit noch **keine offiziell veröffentlichten Übergangsfristen** vor. Um dennoch handlungsfähig zu bleiben, empfiehlt sich folgendes Vorgehen:

- frühzeitig Kontakt mit der jeweiligen Zertifizierungsstelle aufnehmen und die dort geplanten Übergangsregelungen erfragen;
- intern einen realistischen Zeitplan definieren;
- eine Gap-Analyse zur bisherigen ISO/IEC 27701-Version oder zur bestehenden DSGVO-Umsetzung durchführen;
- laufendes Monitoring, ob die österreichische Akkreditierungsstelle offizielle Übergangsmitteilungen veröffentlicht.

PRAXISTIPP

Unternehmen, die ISO/IEC 27701 derzeit nur als Orientierungsrahmen nutzen, profitieren davon, bereits jetzt mit einer schlanken Gap-Analyse zu starten – unabhängig von formalen Fristen.

Fazit

Die eigenständige Ausgestaltung der ISO/IEC 27701 markiert einen wichtigen Schritt hin zu einem realistisch umsetzbaren Datenschutz-Managementsystem – insb für kleine und mittlere Unternehmen. Die neue Fassung senkt zwar die Einstiegshürden, löst sich jedoch bewusst nicht von ihren Wurzeln in der Informationssicherheit.

Gerade diese Kombination macht ihren praktischen Nutzen aus: ISO/IEC 27701 versteht Datenschutz nicht als isolierte Compliance-Disziplin, sondern als **steuerbares Governance- und Risikomanagement-Thema**. Datenschutzrisiken werden nicht pauschal vermieden, sondern systematisch bewertet, dokumentiert und nachvollziehbar behandelt.

Für DBA entsteht dadurch ein wesentlicher Mehrwert: Die Norm setzt ein **strukturiertes Risikomanagement für Datenschutzrisiken voraus** und schafft damit eine belastbare Grundlage für Entscheidungen, die gegenüber dem Management begründet und abgesichert werden können. Die klare Trennung zwischen zulässiger Risikoabwägung und unzulässiger Risikoakzeptanz – insb bei Rechts- und Compliance-Risiken – stärkt die fachliche Rolle des Datenschutzes im Unternehmen.

Als Orientierungsrahmen – auch ohne Zertifizierungsabsicht – unterstützt ISO/IEC 27701 Organisationen dabei, bestehende DSGVO-Umsetzungen zu strukturieren, Prioritäten transparent festzulegen und Datenschutz als **dauerhaften Managementprozess** zu verankern. Damit wird die Norm weniger zum reinen Prüfmaßstab als vielmehr zu einem Instrument für gelebte, praktikable Datenschutz-Governance.

Dako 2026/7

Zum Thema

Über die Autorin

Bettina Sterner, BA, ist Datenschutz- und Governance-Expertin mit Schwerpunkt auf der Umsetzung regulatorischer Anforderungen. E-Mail: bettina.sterner@outlook.com

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste Cybersecurity – Verteidigung und Vorfallsbewältigung

Cyberbedrohungslage; Prozess für Risikomanagement; Sicherheitsvorfall. Cybersicherheit zählt angesichts einer verschärften Bedrohungslage zu den zentralen Herausforderungen moderner Unternehmensführung – auch auf Grund des Einsatzes von KI. Die Checkliste bietet Unternehmen jeder Größe eine praxisgerechte Orientierungshilfe, um bestehende Sicherheitsmaßnahmen, Meldeprozesse und organisatorische Abläufe systematisch zu überprüfen und auf den Stand der Technik zu bringen.

Einleitung

Cybersicherheit zählt zu den zentralen Herausforderungen moderner Unternehmensführung. Die fortschreitende Digitalisierung betrieblicher Prozesse, die zunehmende Nutzung von Cloud-Services, mobilen Endgeräten und Künstlicher Intelligenz sowie eine stetig wachsende Bedrohungslage durch Cyberangriffe verlangen von Unternehmen jeder Größe ein systematisches und nachweisbares Sicherheitsmanagement, das auch den gesetzlichen Anforderungen entspricht.

Die **Cyberbedrohungslage** verschärfte sich im Jahr 2025 deutlich. Sowohl internationale Sicherheitsberichte wie der CrowdStrike Global Threat Report 2025[1] oder der BSI-Lagebericht für Deutschland[2] als auch nationale Analysen wie die KPMG-Cyberstudie 2025 „Cybersecurity in Österreich“[3] sowie der Cybercrimereport 2024 des BMI[4] zeigen, dass Unternehmen

[1] https://kurzlinks.de/3xff. [2] https://kurzlinks.de/ohj6.
[3] https://kurzlinks.de/xqpb. [4] https://kurzlinks.de/tmuo.