ISACA Switzerland Chapter

Nr. 03 | September 2020 | www.isaca.ch

NEWSLETTER

ISO 27001

Neue ISO Norm zur Umsetzung des Datenschutzes in einem Unternehmen Seite 68

ISACA Event

Reise durch Zeit und Raum. ISACA Vorstand Alumni Event und AHS in Luzern Seite 69

ISACA-Training

Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite 71

ISO 27701 – Nachweisbarer Datenschutz?

Von Andreas Wisler

Im August 2019 wurde ohne grosses Aufsehen die ISO 27701 veröffentlicht. Damit kann ein Unternehmen nachweisen, dass es Anstrengungen zur Umsetzung des Datenschutzes umsetzt. Der Standard trägt den offiziellen Namen «Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines». Obwohl die Norm schon über ein Jahr verfügbar ist, sind die ersten Zertifizierungen erst seit wenigen Wochen möglich. Zeit also, sich genauer damit zu beschäftigen.

Der Datenschutz ist schon lange ein Thema. Die OECD hat 1980 die erste Version des Privacy Frameworks herausgegeben. In England wurde der Vorgänge zur heutigen ISO 27701 erstellt, der British Standard BS 10012:2017 mit der Erweiterung A1:2018. Mit dieser Erweiterung ist der Standard kompatibel mit der Datenschutz-Grundverordnung der Europäische Union. International fehlte bis dahin ein Pendant. Zwar war mit der ISO/IEC 27552 ein Grundlagen-Dokument vorhanden, doch das genügte nicht. Im August 2019 war es dann soweit, die ISO 27701 wurde offiziell veröffentlicht.

Doch die ISO 27701 kann nicht für sich allein zertifiziert werden. Die Basis ist immer ISO 27001. Bei diesem Standard geht es darum, ein Informationssicherheits-Management-Systeme, kurz ISMS, aufzubauen, zu unterhalten und weiterzuentwickeln. Zu den bereits vorhandenen Punkten kommen weitere Anforderungen. Die wichtigste Aussage ist etwas versteckt und wird gerne überlesen, hat aber eine enorme Tragweite. Immer wenn im Standard von «information security» geschrieben wird, muss dies durch «information security and privacy» ersetzt werden. Allein diese Ersetzung gibt einiges zu bearbeiten.

Obschon ISO bestimmt hat, dass alle Definitionen in der ISO 27000 gesammelt werden, mussten zwei weitere Begriffe definiert werden. Es handelt sich um den «joint PII controller» (PII steht dabei für Personally Identifiable Information) und um «privacy information management system», kurz PIMS. Der erstgenannte Begriff wird dabei wie folgt definiert: «Verantwortliche für die Verarbeitung personenbezogener Daten, die gemeinsam mit einem oder mehreren anderen Verantwortlichen für die Verarbeitung die Zwecke und Mittel der Verarbeitung bestimmen».

Struktur

Die Struktur orientiert sich an der ISO 27001. In Kapitel 5 werden die notwendigen Erweiterungen zur ISO 27001 definiert. Dabei gibt es nur für die Kapitel 4 (Context of the organization) und Kapitel 6 (Planning) zusätzliche Massnahmen. Doch die haben es in sich. Schon nur die SoA (Statement of Applicability) zu erweitern, gibt einen grossen Aufwand.

In Kapitel 6 folgen die Erweiterungen zu den 114 Controls aus der ISO 27001. Hier ist es gerade umgekehrt. Nur zum Kapitel 17 (Information security aspects of business continuity management) hat es keine Erweiterungen. Glücklicher-

weise sind es aber «nur» 29 erweiterte Controls.

Leider verwendet der Standard den Begriff «Customer» für drei verschiedene Fälle:

- Vertragsbeziehung zwischen Principal (natürliche/betroffene Person) und Controller (Verantwortlicher)
- Vertragsbeziehung zwischen Controller und Processor (Verarbeitet im Auftrag)
- Vertragsbeziehung zwischen Processor und Sub-Processor

Beim Umsetzen gilt es immer alle drei Fälle zu berücksichtigen, je nachdem, in welcher Rolle sich das Unternehmen selbst befindet.

Mit den Erweiterungen ist es aber nicht getan. Das Kapitel 7 definiert zusätzliche 30 Controls, die es umzusetzen gilt, wenn das Unternehmen als Verantwortlicher für die Verarbeitung von personenbezogenen Daten tätig ist. Die Unterkapitel definieren Anforderungen zu «Bedingungen für die Sammlung und Verarbeitung», «Verpflichtungen gegenüber PII-Grundsätzen», «Privacy by design and privacy by default» und «Gemeinsame Nutzung, Übertragung und Offenlegung von PII».

Im Kapitel 8 folgen zusätzliche 18 Anforderungen an den Processor, welcher im Auftrag personenbezogene Daten verarbeitet. Ist ein Unternehmen Verantwortlicher für die Verarbeitung und verarbeitet auch selbst Daten, gilt es beide Kapitel umzusetzen, was zusätzliche 48 Controls bedeutet (beinahe eine Verdoppelung).

Anhänge

Im Unterschied zur ISO 27001 sind die Controls nicht in einem eigenen Standard vorhanden (der ISO 27002), sondern sind direkt in einem Dokument abgedruckt. Dies macht den Standard etwas schwer lesbar. Die Anhänge A und B sind normativ, das heisst verbindlich umzusetzen, während die erwähnten Kapitel 7 und 8 informativ sind. Die Kapitel 7 und 8 entsprechen damit den Anforderungen aus ISO 27002, während die Anhänge A und B dem Anhang A aus ISO 27001 entsprechen.

Die weiteren Anhänge zeigen die Verknüpfung zu anderen Normen. Der Anhang C verbindet die Controls mit der ISO/IEC 29100 (Privacy framework), der Anhang D mit der Datenschutz-Grundverordnung, Anhang E mit der ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) und der ISO/IEC 29151 (Code of practice for personally identifiable information protection) und der Anhang F zeigt, wie die Controls aus ISO/IEC 27701 mit den Standards 27001 und 27002 in Verbindung gebracht werden können.

Wer sich bereits mit der ISO/IEC 29100 auseinandergesetzt hat, wird sicherlich bemerken, dass die beiden Kapitel 5.11 Information Security und 5.12 Privacy Compliance nicht übernommen wurden. Da ISO 27701 ja auf Basis eines ISMS aufgebaut wird, sind diese Themen bereits genügend abgedeckt.

Zertifizierung

Wie kann sich nun ein Unternehmen zertifizieren lassen? In der Schweiz gibt es bis heute keine akkreditierten Stellen. Als oberstes vergibt das IAF (International Accreditation Forum, https://www.iaf.nu/) die Vergabe an die nationalen Stellen. In der Schweiz ist dies die SAS (Schweizerische Akkreditierungs-Stelle, https://www.sas.admin.ch/). Diese wiederum vergibt an Audit-Firmen die Erlaubnis. Während es in den USA bereits eine Handvoll Unternehmen gibt, die eine Prüfung nach ISO 27701 durchführen dürfen, wird es sicherlich noch länger dauern, bis dies bei uns möglich sein wird.

ISACA CDPSE

Auch ISACA war nicht untätig und hat eine neue Zertifizierung auf dem Markt gebracht, den Certified Data Privacy Solutions Engineer, kurz CDPSE. ISACA beschreibt dies wie folgt: «Inhaber dieser Zertifizierung bestätigen ihre Erfahrung und Fähigkeit, umfassende Datenschutzlösungen zu entwickeln und zu implementieren, die die Lücke zwischen den technischen und rechtlichen Aspekten der Einhaltung des Datenschutzes überbrücken. CDPSE-Besitzer können ein gemeinsames Verständnis der Datenschutzpraktiken in der gesamten Organisation fördern, um die ordnungsgemässe Integration von IT-Datenschutzlösungen zu gewährleisten, die Risiken mindern.». Weitere Informationen sind zu finden unter: https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer.

DER AUTOR

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISA, CDPSE, ISO 22301 sowie 27001 Lead Auditor und der erste ISO 27701 Lead Auditor in der Schweiz. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen bei der Erlangung des ISO 27001 und neu des ISO 27701 Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.