TÜV Media

Die ISO/IEC 27701 – das Privacy Information Management System

Gerald Spyra

TÜVRheinland
Genau. Richtig.

IMPRESSUM

Autor

Gerald Spyra

Die Inhalte des E-Books sind zuerst erschienen als Beitrag in unserem aktuellen Praxishandbuch „Information Security Management“.

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7406-0653-4

www.tuev-media.de

Inhalt

Zum Inhalt
Der noch wenig verbreitete Standard ISO/IEC 27701 unterbreitet einen Vorschlag, wie die gesetzlichen Anforderungen des Datenschutzes in ein ISMS implementiert werden können. Er bietet eine Hilfestellung, mit der die immer komplexer werdenden Anforderungen an den „Schutz von Daten“ praxisorientiert und ressourcensparend in einem Privacy Information Management System umgesetzt werden können.
Das E-Book beschreibt die Herangehensweise und Anforderungen der ISO/IEC 27701 zum Aufbau eines Managementsystems, mit dem die einschlägigen datenschutzrechtlichen Vorgaben vollumfänglich gemanagt und dokumentiert werden können.

1 Herausforderungen und Herangehensweise zum Aufbau eines PIMS

Bei dem noch recht unbekannten Standard ISO/IEC 27701[i] handelt es sich um einen Versuch, die vielfach gesetzlich geregelten Anforderungen des Datenschutzes in normativer Weise als Privacy Information Management System (PIMS) in das Informationssicherheitsmangement zu implementieren (vgl. [1], Abschnitt 4.3). Naturgemäß unterscheiden sich jedoch die mannigfaltigen Anforderungen gerade im Datenschutz im internationalen Umfeld sehr. Das wiederum erschwert natürlich eine normative Umsetzung, die weltweit Anwendung finden soll.

Um dennoch das Ziel der normativen Umsetzung (Vereinheitlichung) zu erreichen, die weltweit Geltung beanspruchen kann, distanziert sich die ISO/IEC 27701 zunächst von den bestehenden gesetzlichen Anforderungen im Bereich Datenschutz und nimmt eine eher generische/abstrakte Sichtweise ein. Es wird versucht, die wesentliche Essenz aus diesen gesetzlichen Anforderungen zu extrahieren bzw. die gesetzlichen Regelungen zu generalisieren und in den Kontext der Informationssicherheit zu setzen.

Wie beim Lesen des Standards deutlich wird, liegt ein besonderer Fokus auf der Umsetzung bzw. Ergänzung der in der ISO/IEC 27002 enthaltenen Maßnahmen um die datenschutzrelevanten Aspekte.

Hinweise

Da bisher nur die englische Fassung der ISO/IEC 27701 existiert, wurden für dieses E-Book wesentliche englische Begrifflichkeiten dieser Norm ins Deutsche übersetzt und interpretiert. Dabei wurde sich insbesondere an den Begrifflichkeiten der DSGVO orientiert. Es ist daher durchaus möglich, dass in der deutschen Überführung der ISO/IEC 27701 in das DIN-Regelwerk gewisse Begriffe und Wörter anders übersetzt werden.

In diesem E-Book werden die Begriffe *Norm* und *Standard* wechselnd und synonym verwendet. Die ISO/IEC-Regelwerke werden im internationalen Umfeld allgemein als *Standards* bezeichnet. In deutscher Literatur findet sich zumeist die Bezeichnung *Normen*.