Datenschutz-Zertifizierung nach ISO/IEC 27552

Die DSGVO sieht vor, dass geeignete Zertifizierungen herangezogen werden können mit denen Auftragsverarbeiter die Sicherheit der Verarbeitung nachweisen können. Eine Zertifizierung macht es einem Auftraggeber damit einfacher den Auftrag zu erteilen. Auch hat ggf. eine Zertifizierung nach Art. 83 DSGVO Einfluss auf die Höhe eines möglichen Bußgeldes nach Zwischenfällen. Leider gibt bis heute aber noch keine Zertifizierung, die den Vorgaben des Gesetzes entspricht. Die ISO/IEC 27552 ist dafür aber ein aussichtsreicher Kandidat.

Nutzen einer Datenschutz-Zertifizierung

München, 25.2.2019. Eine Datenschutz-Zertifizierung, die den Vorgaben des DSGVO entspricht, hätte einige Vorteile für Unternehmen. Will z.B. ein Cloud-Dienstleister personenbezogene Daten seiner Kunden verarbeiten, so muss der Auftraggeber die Sicherheit der Verarbeitung bei dem Dienstleister sorgfältig prüfen. In der Praxis geschieht dies durch aufgrund wenig aussagekräftiger Sicherheitskonzepte bzw. Technisch- Organisatorische Maßnahmen. Beider Parteien bewegen sich dort nach meiner Meinung oft auf sehr dünnem Eis, wenn es zu einem Zwischenfall kommen sollte. Sollte es zu einem Zwischenfall kommen, könnte kritisch geprüft werden, ob die Sicherheit der Verarbeitung ausreichend geprüft wurde. Eine Zertifizierung könnte ein geeigneter Nachweis sein, und hätte obendrein den Nebeneffekt, dass es sich nach Art. 83 Abs. 2 j) DSGVO günstig auf die Höhe eines möglichen Bußgelds auswirken würde. Gleichzeitig weisen Geschäftsführer im Rahmen einer Zertifizierung nach, dass sie eine geeignetes Kontrollsystem aufgebaut haben und reduzieren damit ihre Haftung im Falle eine Falles.

Zertifizierungs-Standards

In Art. 42 und 43 DSGVO sind die Randbedingungen für eine solche Zertifizierung beschrieben. Leider gibt es bis heute keine von den Aufsichtsbehörden genehmigte Zertifizierung. Vor der DSGVO war es allgemein anerkannt, dass bereits mit einer Überprüfung eines ISO/IEC 27001 Zertifikates des Auftragnehmers der Auftraggeber seiner Sorgfaltspflicht weitgehend nachgekommen ist. Bei Cloud-Providern gehört ein ISO/IEC 27001 Zertifikat daher seit Langem zum guten Ton. Die ISO/IEC ISO 27552, die augenblicklich im Entwurf vorliegt, könnte eine geeignete Zertifizierung sein diesen Zweck in Zukunft zu erfüllen.

ISO/IEC 27552

Die Norm ISO/IEC 27552 ist Bestandteil der ISO 27000 Familie. Im Englischen Titel heißt sie „Extensions to ISO/IEC 27001 and ISO/IEC 27002 for privacy management - requirements and guidelines“. Sie enthält damit gegenüber der ISO/IEC 27001 neue Anforderungen, und formuliert Empfehlungen zur Umsetzung der ISO 27002, beides unter den Gesichtspunkten des Datenschutzes. Für eine Zertifizierung wären die Anforderungen zusätzlich zu denen der ISO/IEC 27001 heranzuziehen.

Zu den neuen Anforderungen zählen Ergänzungen zu den Hauptkapiteln der Norm. So werden die Anforderungen an das Risikomanagement so ergänzt, dass auch die Datenschutz-Folgenabschätzung enthalten ist. Hinsichtlich der Erklärung zur Anwendbarkeit wird auch gefordert, dass die in der ISO/IEC 27552 in den Anhängen A und B gegebenen neuen Controls analog zu denen des Anhangs A der ISO/IEC 27001 zu berücksichtigen sind.

Darüber hinaus enthält die ISO/IEC 27552 in zusätzliche Maßnahmen und Ziele (49 controls & 6 objectives) welche die der ISO 27001 ergänzen. Diese enthalten, Aufgeteilt nach Anforderungen an Verarbeiter (processor) und an Auftraggeber bzw. verantwortliche Stellen (controller). Dort sind z.B. Verträge zur Verarbeitung im Auftrag angesprochen, Informationspflichten gegenüber Betroffenen, „Privacy by design and default" oder die Offenlegung von Unterauftragnehmern.

Ergänzt werden diese neuen Anforderungen durch Empfehlungen zur Umsetzung von bestehenden Controls. Dabei werden z.B. Empfehlungen zum Vorgehen bei Zwischenfällen angesprochen.

Zuletzt enthält die Norm in den Anhängen Tabellen, die eine Referenz der einzelnen Normabschnitte mit der DSGVO sowie anderen ISO Normen herstellen.

Zusammenfassung

IN der ISO/IEC DIS 27559 sind nach einer ersten Einschätzung zahlreiche Aspekte der Verarbeitung personenbezogener Daten abgedeckt. Die Norm wiederholt dabei nicht alle Einzelheiten des Gesetzes, spricht aber systematisch alle Aspekte der Umsetzung an. Ein Blick in den Gesetzestext wird sich also bei einer Implementierung eines DSGVO-konformen Datenschutzmanagements nicht vermeiden lassen. Einzelne Passagen erscheinen noch verbesserungsfähig und Teile der Referenztabellen wirken nicht in allen Belangen vollkommen schlüssig. Hinsichtlich der Sicherheit der Verarbeitung bietet diese Norm, zusammen mit der ISO/IEC 27001, aber eine umfassende Grundlage für eine Zertifizierung im Sinne des Art. 43 DSGVO. Besonders Firmen aus Branchen in denen ISO/IEC 27001 Zertifizierungen flächendeckend umgesetzt sind, wie bei Automobilzulieferern, Energienetzbetreibern oder Cloud-Dienstleistern, bietet dieses Vorgehen die Chance mit vernünftigem Aufwand ein aussagekräftiges Datenschutzzertifikat zu erhalten. Es bleibt nur noch zu Hoffen, dass die Aufsichtsbehörden dies ähnlich sehen und die Zertifizierung entsprechend anerkennen.

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de

ISO/IEC 27001 Lead-Auditor im Auftrag des TÜV Rheinland u. Deutsche Auditoren eG, Lead-Auditor & Fachexperte IT-Sicherheitskatalog nach §11 Abs. 1a EnWG, Lead Auditor ISO 22301 Business Continuity Management, Auditor für kritische Infrastrukturen gemäß §8a BSIG, VdS-zertifizierter Berater für Cyber-Security, Datenschutzbeauftragter IHK