Datenschutz mit Zertifikat

Zertifizierungen erleichtern das Geschäftsleben. Man weist gegenüber Geschäftspartnern nach, dass man einen hohen Standard einhält. Sollte trotzdem mal etwas schief gehen kann der Geschäftsführer belegen, dass er alles Erforderliche getan hat. Die EU-Datenschutzgrundverordnung sieht die Möglichkeit einer Zertifizierung ausdrücklich vor, aber wie und wo kann man ein solches Zertifikat erhalten?

Zweck einer Datenschutz-Zertifizierung

Einfacher Vertragsschluss zur Verarbeitung im Auftrag

So gut wie jede Firma lässt personenbezogene Daten durch Externe verarbeiten. Sie müssen daher Vereinbarungen zur Verarbeitung im Auftrag nach Art. 28 DSGVO mit ihren Auftragnehmern abschließen. Für den Vertragstext werden zumeist allgemein verfügbare Vorlagen genommen. Die Formulierung der Technisch-Organisatorischen-Maßnahmen (TOM) ist dagegen regelmäßig ein Problem. Selbst von großen Firmen bekomme ich als Datenschutzbeauftragter immer wieder TOM die oberflächlich und ohne jede Aussagekraft sind. Praktisch unmöglich, als Auftraggeber anhand dieser Unterlagen der Pflicht nachzukommen, zu prüfen ob der Auftragnehmer geeignete Garantien zur Einhaltung der Datenschutzvorschriften bietet. Bei halbwegs strikter Auslegung der gesetzlichen Vorgaben müssten hier eigentlich viele Beauftragungen scheitern. Das Gesetz zeigt aber auch einen Ausweg (Art. 28 Abs. 5), da eine Zertifizierung des Auftragnehmers gemäß Art. 42 DSGVO herangezogen werden kann um die geforderten Garantien nachzuweisen.

Geringeres Bußgeld nach Zwischenfällen

Zwischenfälle passieren, das lässt sich nie ganz verhindern. Einer der wesentlichen Gründe, warum die DSGVO für so viel Wirbel gesorgt hat, liegt in der Höhe der möglichen Bußgelder. Bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Umsatzes, was auch immer höher ist, schreckt gleichermaßen große wie kleine Unternehmen. Wenn eine Firma eine gültige Zertifizierung besitzt und damit nachweisen kann alle erforderlichen Maßnahmen getroffen zu haben, kann sie jedoch gemäß Art. 83 DSGVO mit einem geringeren Bußgeld rechnen. Auch kann die Haftung der Geschäftsführung in diesem Fall anders ausfallen, da grobe Fahrlässigkeit oder Organisationsversagen ausgeschlossen werden kann.

Zertifizierungs-Standards

Datenschutzzertifikate findet man bei verschiedenen Datenschutz Verbänden oder Zertifizierungsunternehmen wie dem TÜV Rheinland. Jedoch erfüllt Keines die Anforderungen der DSGVO. Stand Februar 2019 ist noch keine Zertifizierungsstelle oder und kein Zertifizierungs-Standard offiziell zugelassen.

ISO 27001

Vor Einführung der DSGVO nahm die ISO/IEC 27001 Zertifizierung eine wichtigere Rolle ein. Es war allgemein anerkannt, dass bei einer Beauftragung der Auftraggeber mit einer

Überprüfung eines solchen Zertifikates seiner Sorgfaltspflicht weitgehend nachgekommen ist. Allerdings enthält die ISO/IEC 27001 neben einem allgemeinen Vermerk zum Datenschutz keine konkreten Vorgaben zur DSGVO. Für Cloud-Dienstleister gibt es daneben schon länger die Ergänzungen ISO 27017 und ISO 27018. Neben den großen Anbietern wie Apple, Microsoft, Amazon und Google haben sich bisher wenige Cloud Provider, wie z.B. netfiles, dieser Ergänzungen angenommen.

ISO 27522

Mit der ISO/IEC 27522 befindet sich ganz aktuell eine Ergänzung zur ISO 27001 in der finalen Abstimmung, die das Thema Datenschutz allgemein aufgreift und auch ausdrückliche Referenzen auf die DSGVO enthält.

Der neue Standard ergänzt die bestehende ISO 27001 an verschiedenen Stellen, wobei jeweils genau angegeben ist, welche Teile der ISO 27001 unverändert weiter gelten und an welchen Stellen Ergänzungen angebracht werden. So wird das Thema Risikomanagement ergänzt, unter anderem um die Datenschutzfolgenabschätzung (Art. 35 DSGVO). Auch zu den Maßnahmen aus dem Anhang A der ISO 27001 bzw. der Anleitung zur Umsetzung ISO/IEC 27002 gibt es zahlreiche Ergänzungen. Dies sind zum Teil spezifische Hinweise zur Umsetzung der bestehenden Maßnahmen, aber auch ganz neue Maßnahmen. Sowohl für Auftraggeber als auch für Verarbeiter personenbezogener Daten. An verschiedenen Stellen findet man dabei den Wortlaut der DSGVO wieder. Z.B. findet sich im Kapitel 7.2.2 des Standards die Aufzählung der Grundlagen der Rechtmäßigkeit der Verarbeitung aus DSGVO Art. 6 Abs. 1 a) – f). Auch zahlreiche andere Aspekte der DSGVO, wie Verarbeitung im Auftrag, Verzeichnis der Verarbeitungstätigkeiten und „privacy by design“ finden sich in den ergänzenden Maßnahmen. Zuletzt haben sich die Ersteller der Norm noch die Mühe gemacht eine Referenztabelle zwischen der ISO 27522 und der DSGVO sowie der ISO 27017 und 27018 zu erstellen.

Für die zahlreichen Unternehmen, die heute schon eine ISO 27001 Zertifizierung besitzen, kann die ISO 27522 eine sinnvolle Ergänzung sein, um die Einhaltung der Datenschutz-Grundverordnung DSGVO gegenüber Kunden, Partnern und Behörden nachzuweisen. Sie lässt sich einfach in das bestehende Schema integrieren und im Rahmen des regelmäßigen ISO 27001 Audits zertifizieren.

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