Datenschutz-Management-System: Zertifizierung Compliance-Kit 2.0

Seit dem 6. August 2019 verfügt die IITR Datenschutz GmbH über eine Bestätigung, wonach das Compliance-Kit 2.0 die Vorschriften der DSGVO umfassend und korrekt abbildet. Diese Bestätigung wurde von den staatlich geprüften und beeideten Ziviltechnikern Herrn Dipl.-Ing. Dr. Peter Gelber und Herrn Dipl.-Ing. Wolfgang Fiala ausgestellt und ist einer amtlichen Prüfung gleichzustellen.

Ziviltechniker (Quelle: https://de.wikipedia.org/wiki/Ziviltechniker) sind gemäß einer österreichischen Bestimmung als „Personen öffentlichen Glaubens“ befugt, bestehende Übereinstimmungen zu überprüfen und darüber Urkunden auszustellen.

Zur Prüfung wurde das Compliance-Kit 2.0 (Quelle https://www.iitr.de/produkte-services/compliance-kit.html) vorgelegt. Die Untersuchung ist in einem Prüfgutachten (Quelle: https://www.iitr-cert.com/) dokumentiert, die Bestätigung der Übereinstimmung liegt als Urkunde (Quelle: https://www.iitr-cert.com/) vor. Damit erhält das Compliance-Kit 2.0 seine offizielle Anerkennung.

Das Compliance-Kit 2.0 ist als Datenschutz-Management System angelegt.

Zertifizierung auf Basis eines Datenschutz-Management-Systems

In der Fachliteratur wird vielfach darauf hingewiesen, dass ein Datenschutz-Management-System das geeignete Instrument schlechthin darstellt (vgl. TeleTrust, Handreichung zum Stand der Technik, S. 71, Zitat am Ende und Jung, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208, Zitat am Ende), um die Anforderungen der DSGVO und hierbei insbesondere die Vorgaben der Rechenschaftspflicht zu erfüllen.

Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss hat entschieden, dass in Art. 42 DSGVO nach seiner Lesart eine Zertifizierung von Management-Systemen nicht vorgesehen sei. Wohl auch in Folge darauf hat die deutsche Zertifizierungsbehörde DAkkS ihrerseits nun Richtlinien veröffentlicht, die sich ausschließlich mit der Zertifizierung von Produkten und Dienstleistungen befassen (vgl. hierzu „Die Zertifizierung nach der DSGVO: Innovatives, aber hochkomplexes Instrument“, DuD 8/2019, Dr. Natalie Maier, LL.M. und Tamer Bile, LL.M., Wissenschaftliches Zentrum für Informationstechnik-Gestaltung an der Universität Kassel, https://link.springer.com/article/10.1007/s11623-019-1147-x).

Einen weiteren Überblick über den Sachverhalt ermöglicht der Artikel von Herrn Oliver Schonschek (Quelle: https://www.computerwoche.de/a/welche-datenschutz-zertifikate-passen-zu-dsgvo-und-gdpr,3545410).

Compliance-Kit 2.0 als Basis

Wir haben uns entschieden, unseren Mandanten ein Datenschutz-Management-System sowie die Möglichkeit einer eigenen Zertifizierung anzubieten. Diese Zertifizierung wird durch die IITR Cert GmbH (Quelle: https://www.iitr-cert.com/) vorgenommen, zu diesem Zweck als eigenständige Prüfstelle installiert.

Aufgrund der Beurkundung durch Ziviltechniker als einer dazu berechtigten Stelle steht den Unternehmen mit dem Compliance-Kit 2.0 ein qualifiziertes Instrument zur Verfügung, eine Übereinstimmung mit der DSGVO herzustellen und sich bestätigen lassen zu können.

Zertifizierungsstellen

Gemäß einer EU-Norm (Verordnung (EG) Nr. 765/2008, Artikel 4 Abs. 1, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:de:PDF) waren bis zum Inkrafttreten der DSGVO die nationalen Zertifizierungsstellen alleine für Zertifizierungen innerhalb ihres jeweiligen Staates zuständig (in Deutschland ist dies die DAkKS). Durch die DSGVO entstand hier eine neue Lage, indem sie bestimmte Vorgänge im Bereich von Zertifizierungen für sich reklamiert. Datenschutzbehörden eines Landes sind seitdem in den hoheitlichen Vorgang der Zertifizierung für den Bereich Datenschutz zusätzlich eingebunden. Die föderal organisierte Bundesrepublik Deutschland verfügt über Landesdatenschutzbehörden, die sich diesbezüglich intern abstimmen. Die stimmberechtigte Vertretung Deutschlands auf EU-Ebene geschieht im Europäischen Datenschutzausschuss und liegt in den Händen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Ausweichmöglichkeit für Groß-Unternehmen

Derzeit ist die Begutachtung eines Unternehmens nur mittelbar über den Umweg einer Zertifizierung der eigenen IT-Sicherheit nach ISO 27001/27002 („Informations-Sicherheits-Management“) möglich, auf welche sodann künftig eine Mit-Zertifizierung nach ISO 27701 (Quelle: https://www.iso.org/standard/71670.html) für den Bereich Datenschutz aufgesetzt werden kann (wobei auch dies letztlich keine „Zertifizierung“ im Sinne von Artikel 42 DSGVO darstellt).

Diese Verfahrensweise ist nur durch Groß-Unternehmen durchführbar oder aber bei Einheiten, deren Geschäftstätigkeit eine extreme Datensensibilität aufweist und aus diesem Grunde die erheblichen Mittel aufzubringen hat, sich nach diesen Normen überprüfen zu lassen.

Für die Vielzahl der Unternehmen kann diese Vorgehensweise aus vielen Gründen schlichtweg nicht in Betracht kommen. Zunächst ist es viel zu teuer, hier ist die Rede von 5-stelligen Euro-Beträgen aufwärts. Weiterhin sind Fachleute, die solche Zertifizierungen durchführen könnten, in genügender Zahl gar nicht verfügbar.

Rechenschaftspflicht und Datenschutz-Management-System

Über die Notwendigkeit, ein Datenschutz-Management-System zu verwenden sollte es anhand der Anforderungen der DSGVO (Rechenschaftspflichten) keine Zweifel geben. So sieht dies auch die Unternehmensberatung KPMG (Quelle: https://klardenker.kpmg.de/datenschutz-managementsystem-pruefung-bringt-sicherheit/). Für den Fall, dass ein Unternehmen auf softwaregetriebene Strategien zur Bewältigung der Datenschutz-Anforderungen zurückgreifen will – was sich ab einer bestimmten Größe eines Unternehmens nicht wird vermeiden lassen – wird parallel dazu die Führung eines Datenschutz-Management-System angezeigt sein, schon weil die Geschäftsführung über die erfolgte Umsetzung der Bestimmungen schriftliche Erklärungen abzugeben hat. Schließlich befindet sich die Geschäftsführung in Haftung für die tatsächliche Umsetzung und wird sich dabei nicht auf die korrekte Installation und Arbeitsweise einer Software verlassen wollen.

Leistungsumfang des Compliance-Kit 2.0

Dieses fasst zunächst die Bestimmungen der DSGVO zusammen und stellt diese der ISO High Level Structure folgend zur Verfügung. Das Compliance-Kit 2.0 ähnelt damit beispielsweise einer BS 10012 der BSI Britisch Standard Institution. Die Ähnlichkeit verwundert nicht, da beiden inhaltlich dieselbe DSGVO zugrundeliegt, die BS 10012 umfasst allerdings zusätzlich einige britische Besonderheiten.

Darüber hinaus muss ein Datenschutz-Management-System die in der DSGVO konkretisierten Forderungen hinsichtlich der Dokumentation von Beschreibungen sowie die Hinterlegung abzuschließender Verträge ermöglichen und diese Vorstellungen in einer nachvollziehbaren, daher versionierenden Weise archivieren können. Nützlich erweisen sich zahlreiche Vorlagen, die an den betreffenden Stellen durch ein Management-System zur Verfügung gestellt werden. Eine eLearning-Plattform ist integriert, um die bestehende Verpflichtung der Sensibilisierung aller Mitarbeiter für die Belange des Datenschutzes durch den Datenschutzbeauftragten des Unternehmens vornehmen zu können. Absolvierte Schulungen müssen nachweisbar sein und werden durch das Management-System dokumentiert.

Vorteile der Zertifizierung

Gerade im Datenschutz sind bei Austausch von personenbeziehbaren Daten die Voraussetzungen einer unternehmensübergreifenden Zusammenarbeit und Auftragsvergabe rigiden Bedingungen unterworfen worden. Teilweise wurde eine faktische Beweislastumkehr eingeführt, die Haftung für korrektes Verhalten eines Auftragnehmers reicht dabei zurück auf die Geschäftsleitung des Auftraggebers.

Wer wollte da nicht gerne auf eine möglichst zutreffende Aussage und Bewertung der datenschutzrechtlichen Strukturen seines potentiellen Auftragnehmers zurückgreifen.

Für einen potentiellen Auftragnehmer wiederum könnte es vorteilhaft sein, dem zukünftigen Auftraggeber ein Zertifikat vorlegen, um seine eigenen Bemühungen zu datenschutzrechtlich korrekten Strukturen belegen zu können.

Auch nach innen wirkt eine Zertifizierung. Man erhält Sicherheit, in diesem Bereich korrekt aufgestellt zu sein. Man folgt Standards, die jenen entsprechen, die auch der Geschäftspartner anwendet.

Kunden mögen es, durch gut strukturierte Unternehmen betreut zu werden. Kaum ein Kunde dürfte ein Unternehmen vorziehen, weil es kein Zertifikat aufweisen kann.

Dergleichen wirkt auf die eigenen Mitarbeiter. Zertifizierung im Datenschutz hat sowohl eine Schutz- als auch Signal-Wirkung nach innen wie auch nach außen.

Position der EU-Kommission

Amtliche Zertifizierungen für Management-Systeme stehen wie geschildert derzeit nicht zur Verfügung. Es werden lediglich Produkte und Dienstleistungen zertifiziert. Die EU-Kommission schreibt am 24. Juli 2019 dazu (Quelle: https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf):

> „Businesses are adapting their practices (…)
>
> Finally, certification can also be a useful instrument to demonstrate compliance with specific requirements of the Regulation. It can increase legal certainty for businesses and promote the Regulation globally. The certification and accreditation guidelines recently adopted by the European Data Protection Board will enable the development of certification schemes in the EU. The Commission will be monitoring these developments and, if appropriate, will make use of the empowerment provided under the Regulation to frame the requirements for certification. The Commission may also issue a standardisation request to EU standardisation bodies on elements relevant for the Regulation."

Fazit

Wir danken Herrn Dipl.-Ing. Dr. Peter Gelber (Quelle: http://www.dsgvo-zt.at/) und Herrn Dipl.-Ing. Wolfgang Fiala (Quelle: http://www.dsgvo-zt.at/). Diese hatten als Ziviltechniker die Sichtung eines umfangreichen Datenschutz-Management-Systems durchzuführen und zu beurteilen. Wir danken ferner Herrn Zlamal, Geschäftsführer der IITR Cert GmbH (Quelle: https://www.iitr-cert.com/), für sein außerordentliches Engagement.

Wir sind überzeugt, dass ein Datenschutz-Management-System das geeignete Instrumentarium für Unternehmen und verwandte Wirtschafts-Strukturen zur Verfügung stellt, um den komplexen Anforderungen der DSGVO entsprechen zu können. Diese Überzeugung entspringt unseren eigenen Erfahrungen in den durch uns betreuten Unternehmen. Ausdrücklich bestätigen wir diesbezügliche Empfehlungen und Analysen aus Wirtschaft und Forschung.

Der Umstand, derzeit nicht auf staatliche Zertifizierungen nach der DSGVO von Datenschutz-Management-Systemen zurückgreifen zu können, darf aus unserer Sicht nicht dazu führen, zertifizierte Datenschutz-Management-Systeme dem Markt vorzuenthalten. Hier sehen wir uns als Privatunternehmen gefordert.

Das Compliance-Kit 2.0 steht als Grundlage einer qualifizierten Ermittlung der Übereinstimmung mit den Bestimmungen der DSGVO für alle Interessenten zur Verfügung.

Autor: Eckehard Kraska

Kontakt: Rechtsanwalt Dr. Sebastian Kraska, externer Datenschutzbeauftragter

Internet: www.iitr.de

Telefon: 089-18 91 73 60

E-Mail: email@iitr.de

Stand: 7. August 2019

Quellen/Zitate:

TeleTrust, Handreichung zum Stand der Technik, S. 71, Quelle: https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf

Kontext Datenschutz

Auch im Hinblick auf die Überprüfung der Wirksamkeit von Maßnahmen im Zusammenhang mit den Anforderungen nach der DSGVO bietet sich die Implementierung eines Managementsystems – genauer: eines Datenschutz-Managementsystems (DSMS) – an. Zwar schreibt die DSGVO ein solches nicht ausdrücklich vor. Sie lässt gleichwohl aber an vielen Stellen die Notwendigkeit eines DSMS erkennen. So verlangt beispielsweise Art. 32 Abs. 1 lit. d) DSGVO ein „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung".

Da ein solches Verfahren innerhalb der Organisation ein geplantes und strukturiertes Vorgehen erfordert, mithin also eine Umsetzung des klassischen PDCA-Modells bedingt, bietet sich hierfür die Einrichtung eines DSMS geradezu an. Wird dieses an den Elementen der ISO-High-Level-Structure ausgerichtet, kann es zudem in ein bereits vorhandenes ISMS auf Basis ISO 27001 integriert werden.

Genauso wie ein ISMS lässt sich dann auch das DSMS auditieren und damit sukzessive der Reifegrad des Systems feststellen. Orientiert am Leitfaden ISO 19011 können, auf Basis eines Auditprogramms und eines Auditplans, Audits durchgeführt werden. Die Durchführung von Audits kann vom Datenschutzbeauftragten vorgenommen werden. Bei größeren Organisationen können Audits auch durch fachkundig geschulte Beschäftigte der Organisation oder auf Datenschutz spezialisierte Beratungsunternehmungen erfolgen.

Jung, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208, Quelle: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2018%2Fcont%2Fzd.2018.208.1.htm&anchor=Y-300-Z-ZD-B-2018-S-208-N-1

Compliance-Management-Systeme (CMS) sind in der heutigen Zeit schon beinahe ein „alter Hut". Dies liegt allein darin begründet, dass es diverse Standards gibt, die den Aufbau eines entsprechenden Systems samt dessen Bestandteilen vorgeben. Anders sieht dies bezogen auf Datenschutzmanagementsysteme (DSMS) aus, wo dem Verantwortlichen zwar durch die Datenschutzgrundverordnung (DS-GVO) entsprechende Rechenschaftspflichten für seine Datenverarbeitungen zugewiesen werden, aber offen bleibt, wie er die Einhaltung der datenschutzrechtlichen Vorschriften konkret nachweisen können muss. Der Beitrag möchte die Notwendigkeit eines DSMS oder zumindest den systematischen Nachweis ordnungsgemäßer Datenverarbeitung darstellen, wobei auch Bezug auf die „alte" Rechtslage bis zum 25.5.2018 genommen wird. Hierbei sollen Ansätze aufgezeigt werden, wie in Ermangelung klarer Standards doch ein vernünftiger Ansatz gewählt werden kann, um den Nachweispflichten, die durch die DS-GVO abverlangt werden, nachzukommen.