Tobias S. Potthoff, Dorothee Schrief

Geschäftsrelevanz Datenschutz spezifischer Zertifizierungen

Befunde einer Befragung in einer multinationalen Unternehmensgruppe der Telekommunikationsbranche

Die Autoren stellen die Ergebnisse einer von Management-Interviews begleiteten Online-Befragung von Datenschutzverantwortlichen einer TK-Unternehmensgruppe zur Verbreitung von und dem Interesse an Datenschutz spezifischen Zertifizierungen vor.

1 Ausgangslage

Mit der im August 2019 vorgestellten Version 1 einer ISO/IEC 27701 werden die global anerkannten Zertifizierungsstandards der ISO-Familie erstmals um eine Zertifizierung für Datenschutzmanagementsysteme („Privacy Information Management Systems" – PIMS) ergänzt, die für die im Rahmen des Informationssicherheitsmanagementsystems (ISMS) verarbeiteten personenbezogenen Daten gelten.[1] Die ISO/IEC 27701 stellt eine Ergänzung der ISO/IEC 27001 f. dar und setzt die Erfüllung der Anforderungen dieses Standards an das Informationssicherheitsmanagementsystem voraus. Erste Zertifizierungen gemäß ISO/IEC 27701 werden für Anfang 2021 erwartet.

Der europäische Gesetzgeber hat daneben in der Datenschutz-Grundverordnung (DSGVO) in Art. 42 f. DSGVO ausdrücklich die Einführung von Zertifizierungen und Prüfzeichen geregelt, um die Transparenz hinsichtlich der Einhaltung von Anforderungen aus der DSGVO zu verbessern und deren Einhaltung zu fördern.[2] In Deutschland ist die Antragsphase für eine Programmprüfung von Konformitätsbewertungsprogrammen im Bereich Datenschutz seit Anfang 2019 bei der hierfür zuständigen Deutsche Akkreditierungsstelle GmbH (DAkks) eröffnet.[3] Die Akkreditierung eines Zertifizierungsverfahrens gemäß Art. 42 DSGVO lässt gleichwohl noch auf sich warten und wird nach Wirksamwerden der DSGVO in 2018 frühestens Anfang 2021 erwartet.[4] Ein Grund für die zeitliche Verzögerung mag das neue Zusammenspiel der unterschiedlichen Interessengruppen sein (u. a. Europäischer Datenschutzausschuss, nationale Datenschutzbehörden und DAkks), das sich erst noch finden muss. Daneben gehen die Auswirkungen der COVID-19 Pandemie auch an den Akkreditierungsprozessen nicht spurlos vorbei.

ISO/IEC 27701 sowie Zertifizierungen gemäß Art. 42 DSGVO stellen dabei nach ganz herrschender Auffassung ein „aliud" mit ganz unterschiedlichen Zertifizierungsgegenständen dar (übergreifendes Datenschutzmanagementsystem für die ISO 27701 vs. konkrete Produkte, Dienstleistungen und Prozesse für Art. 42 DSGVO).[5]

Nach nunmehr über zwei Jahren DSGVO-Wirksamkeit werden Stimmen aus der Wirtschaft laut, die verstärkt zeitgemäße datenschutzspezifische Zertifizierungsstandards einfordern, um die Transparenz digitaler Angebote hinsichtlich der Einhaltung von Datenschutzbestimmungen (insbesondere DSGVO-Anforderungen) zu erhöhen und den Markteilnehmern so endlich eine Orientierungshilfe an die Hand zu geben.[6]

1 Dr. Aleksandra Sowa/Martin Rost: Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO in: DuD 10/2020, S. 659 ff.

Tobias S. Potthoff EMBA (St. Gallen)

ist Rechtsanwalt und Senior Privacy Manager im Bereich Group Privacy bei der Deutsche Telekom AG in Bonn.

E-Mail: Tobias.Potthoff@telekom.de

Dorothee Schrief, M. A.

ist Rechtsanwältin und Leiterin Privacy Audits & Standards im Bereich Group Privacy bei der Deutsche Telekom AG in Bonn.

E-Mail: Dorothee.Schrief@telekom.de

2 Lepperhoff in Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 42 RN 1.

3 https://www.dakks.de/content/projekt-datenschutz.

4 Auskunft Deutsche Akkreditierungsstelle GmbH vom 29. Juni 2020.

5 So auch eine Auskunft von der Landesbeauftragten für Datenschutz und Informationssicherheit Nordrhein-Westfalen nach Anfrage im Juni 2020.

6 *Dr. Claus-Dieter Ulmer*: Europa braucht endlich eine Datenschutz-Zertifizierung auf: https://www.telekom.com/de/konzern/management-zur-sache/details/europa-braucht-endlich-eine-datenschutz-zertifizierung-601144. Vgl. auch *Alisha Gühr/Irene Karper/Sönke Maseberg*: Der lange Weg der Akkreditierung nach Art. 42 DSGVO, Ziffer 6 Wünsche, S. 653 in: DuD 10/2020, S. 649 ff.

2 Einleitung

Im Kontext von Datenschutz-Compliance stellt sich für Datenschutzverantwortliche sowie Datenschutzbeauftragte besonders die Frage nach der spezifischen Geschäftsrelevanz neuer Zertifizierungsangebote im Datenschutzbereich für die jeweiligen Wirtschaftssektoren und Geschäftsfelder. Die Verfasser haben hierzu ergänzend zu einer Online-Marktrecherche unternehmensinterne Befragungen in einer multinationalen Unternehmensgruppe der Telekommunikationsbranche organisiert, um den Kenntnis- und Umsetzungsstand sowie das Meinungsbild von Interessengruppen im Unternehmen zum Bestehen, Nutzen, Kundenerwartungen und zur Machbarkeit datenschutzspezifischer Zertifizierungen empirisch zu erfassen.

Kern der Befragungen war dabei eine betriebs-, unternehmens- und segmentübergreifende Online-Umfrage im Oktober 2020, die sich an zentrale und dezentrale Datenschutzansprechpartner sowie datenschutz- und zertifizierungsnahe Interessengruppen aus unterschiedlichsten Geschäftsfeldern innerhalb der Unternehmensgruppe im In- und Ausland richtete (insgesamt 442 Kontakte).

Die Online-Umfrage haben die Verfasser mit einer internationalen Abfrage bei lokalen Datenschutzbeauftragten (57 Data Protection Officers – DPOs in über 86 Unternehmen[7]) zum Stand lokaler datenschutzspezifischer Zertifizierungsangebote sowie selektive Management-Interviews auf Ebene von Geschäfts- und Budgetverantwortlichen flankiert. Damit wurde ein breites und gut abgestütztes Meinungsbild ermittelt. Die Ergebnisse der Befragungen sowie eine Einordnung und ein Ausblick sind Gegenstand dieser Betrachtung.

3 Ergebnisse der Online-Befragung

3.1 Rücklauf

Die freiwillige und anonyme Online-Umfrage erreichte eine aussagekräftige Rücklaufquote von 32% (140 verwertbare Rückmeldungen von 442 Kontakten). Die Rückläufer kamen dabei zum Großteil aus der Funktion des Datenschutzes (54%), gefolgt von Sicherheit (23%), Sonstige mit den Funktionen Einkauf und Vertrieb (13%), IT (6%) sowie Personal (4%).

3.2 Basiserfassung

Der erste Fragenkomplex der Online-Befragung behandelte die Fragen nach dem Bestehen zertifizierter Managementsysteme und dem Umfang bereits existierender Budgetbereitstellung für Zertifizierungen. Die Teilnehmer haben das Vorliegen folgender Zertifizierungen von Managementsysteme in ihrer Organisationseinheit gemeldet (Top 3): 88x ISO/IEC 27001 (ISMS), 70x DIN EN ISO 9001 (Qualitätsmanagement) und 45x ISO/IEC 20000 (IT Service Management). Das Ergebnis zur weitflächigen Verbreitung von ISO/IEC 27001-Zertifizierungen hat insbesondere für die Einschätzung eines Umsetzungsaufwands für eine Einführung von ISO/IEC 27701-Zertifizierungen Relevanz, da sich diese für Organisationseinheiten, die bereits ISO/IEC 27001 zertifiziert sind, als eine Art „low hanging fruit" und damit als „quick win" darstellen kann. Demgegenüber stehen Organisationseinheiten, die noch keine ISO/IEC 27001-Zertifizierung aufweisen können, aber eine ISO/IEC 27701-Zertifizierung anstreben, vor der großen Herausforderungen, auch eine vollumfängliche ISO/IEC 27001-Zertifizierung umzusetzen. Für solche Organisationseinheiten ohne ISO/IEC 27001-Zertifizierung besteht mithin eine beträchtlicher Umsetzungsaufwand.

Die Rückmeldungen zur Budgetbereitstellung zeigten, dass sich bestehende Zertifizierungen, insbesondere Zertifizierungen von Managementsystemen, im Großteil über ein zentrales Budget finanzieren und damit auf Dachzertifikate schließen lassen, was in einem vielschichtigen und multinationalen Unternehmen opportun erscheint und wirtschaftlich vorteilhaft ist.

3.3 Kernfragen

Der nächste Fragenkomplex erfasste als Kernfragen den Meinungsstand der Teilnehmer über mögliche Bewertungskriterien zur Evaluierung der Stärken und Vorteile einer Datenschutz-Zertifizierung, Kenntnis und Bewertung einschlägiger Standards für Datenschutz-Zertifizierungen sowie eine Abfrage geplanter bzw. denkbarer Gegenstände für eine Datenschutz-Zertifizierung. Als entscheidende Bewertungskriterien für eine Datenschutz-Zertifizierungen nannten die Teilnehmer (Top 5):

- Nachweis der Einhaltung der DSGVO-Pflichten (in Summe 85% „Äußerst wichtig" und „Sehr wichtig"),
- Qualitätsmanagement für Datenverarbeitungsprozesse (in Summe 67% „Äußerst wichtig" und „Sehr wichtig"),
- Exculpation/Bußgeldentlastung (in Summe 66% „Äußerst wichtig" und „Sehr wichtig"),
- Ausschreibungsvoraussetzung (in Summe 85% „Äußerst wichtig" und „Sehr wichtig"),
- Marketing-Effekt (in Summe 85% „Äußerst wichtig" und „Sehr wichtig").

Als vorteilhafte Standards für Datenschutz-Zertifizierungen sehen die Teilnehmer den ISO/IEC 27701-Standard (74%), die in Art. 42 DSGVO vorgesehenen Zertifizierungsstandards (59%) sowie die IDW PS 980[8] (21%). 5% der Teilnehmer benannten „Andere" Standards und 14% der Teilnehmer waren Standards für Datenschutz-Zertifizierungen nicht bekannt. Mehrfachnennungen waren möglich.

Als geplanter bzw. denkbarer Gegenstand für eine Datenschutz-Zertifizierung wurden von den Teilnehmern am häufigsten das unternehmensinterne Privacy & Security Assessment Verfahren[9] (17 Nennungen) gefolgt vom Datenschutzmanagementsystem (13 Nennungen) angegeben. Daneben gab es zahlreiche Einzelnennungen von Bereichen, Prozessen und Produkten als potentielle Zertifizierungsgegenstände.

7 Davon insbesondere auch Beteiligungen in folgenden EU-Mitgliedsstaaten: Österreich, Kroatien, Tschechische Republik, Frankreich, Griechenland, Ungarn, Niederlande, Rumänien und Slowakei.

8 Institut der Wirtschaftsprüfer, Prüfungsstandard 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen.

9 Das Privacy & Security Assessment ist ein unternehmensinterner Prozess, der eine frühe Einbindung von Datenschutz und Informationssicherheit in die Produkt-, System- und Anwendungsentwicklungsprozesse des Unternehmens sicherstellt.

3.4 Abschlussfragen

Der abschließende Fragenkomplex befasste sich mit wahrgenommenen Kundenerwartungen sowie der Bereitschaft, Budget für eine Datenschutz-Zertifizierung bereit zu stellen. Die weitaus meisten Übereinstimmungen der von den Teilnehmern wahrgenommenen Kundenerwartungen betreffen ein hohes Datenschutz- und Informationssicherheitsniveau (24 Nennungen), Datenschutz-Compliance (11 Nennungen) sowie eine Datenschutz-Zertifizierung als Ausschreibungsvoraussetzung (11 Nennungen). Demgegenüber haben drei Teilnehmer übereinstimmend Datenschutz-Zertifizierung ausdrücklich noch nicht als aktuelle Ausschreibungsvoraussetzung wahrgenommen. Ein weiteres Indiz dafür, dass der Markt für datenschutzspezifische Zertifizierungen noch in Entwicklung ist. Weitere Übereinstimmungen betreffen „Internationale Standards, insb. ISO/IEC 27001/TISAX" sowie „Sicherheit geben und Risiken reduzieren, insb. Bußgeldrisiken".

Zur Frage der Budgetbereitstellung für eine Datenschutz-Zertifizierung war nur ein geringer Anteil der Befragten auskunftsbereit (29%). Davon lehnten 13% eine Budgetbereitstellung für eine Datenschutz-Zertifizierung ab. Weitere 15% der Teilnehmer, die sich eine Budgetbereitstellung für eine Datenschutz-Zertifizierung vorstellen können, haben eine Folgefrage zur Höhe des zu bereitstellenden Budgets exklusive interner Entwicklungs- und Umsetzungskosten dahingehend beantwortet, dass sie mehrheitlich (8x bis 50.000 € p.a. und 5x bis 100.000 € p.a.) eine Budget-Bereitschaft in Höhe von maximal 100.000 € p.a. für Datenschutz-Zertifizierungen exklusive interner Entwicklungs- und Umsetzungskosten feststellten. Insbesondere diesen Teil der Online-Umfrage suchten die Verfasser im Wege der flankierenden Management-Interviews auf Ebene von Geschäfts- und Budgetverantwortlichen zu plausibilisieren und zu untermauern.

4 Ergebnisse weiterer Befragungen

4.1 Abfrage bei lokalen Datenschutzbeauftragten zum Stand lokaler Zertifizierungsangebote

Eine parallel zur Online-Befragung vorgenommene Abfrage bei lokalen Datenschutzbeauftragten Data Protection Officers – DPOs zum Stand lokaler datenschutzspezifischer Zertifizierungsangebote hat ergeben, dass ISO/IEC 27001 f. (ISMS)-Zertifizierungen bereits weitreichend im In- und Ausland in der Unternehmensgruppe umgesetzt sind, insbesondere im Umfeld der Geschäftsbeziehungen mit anderen Unternehmen (B2B-Markt). Wie

Springer Vieweg

springer.com/informatik

Testmanagement

O. Droste, C. Merz
Testmanagement in der Praxis
2019, XX, 230 S. 27 Abb., 17 Abb. in Farbe. Geb.
€ (D) 44,99 | € (A) 46,25 | *CHF 50.00
ISBN 978-3-662-49652-7
€ 34,99 | *CHF 40.00
ISBN 978-3-662-49653-4 (eBook)

F. Witte
Testmanagement und Softwaretest
Theoretische Grundlagen und praktische Umsetzung
2., erw. Aufl. 2019, XV, 300 S. 39 Abb. in Farbe. Book + eBook. Brosch.
€ (D) 38,00 | € (A) 39,77 | *CHF 42.00
ISBN 978-3-658-25086-7
€ 29,99 | *CHF 33.50
ISBN 978-3-658-25087-4 (eBook)

Ihre Vorteile in unserem Online Shop:
Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich. * : unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Jetzt bestellen auf springer.com/informatik oder in der Buchhandlung

Part of SPRINGER NATURE

A85548

bereits erläutert[10] ist diese Information für das Anstreben einer ISO/IEC 27701 Zertifizierung des Datenschutzmanagementsystems (PIMS) relevant, zumal sich letztere als Erweiterung einer bereits bestehenden ISO/IEC 27001 f. Zertifizierung mit überschaubarem Aufwand realisieren lässt (sog. „quick win" und „low hanging fruit"). Für zwei Beteiligungsgesellschaften sind sogar schon erste ISO 27701-Pilotierungszertifizierung in Planung und sollen Anfang 2021 umgesetzt werden. Die Rückläufer aus den europäischen Beteiligungsgesellschaften haben gezeigt, dass lokale Art. 42 DSGVO Zertifizierungsangebote – so wie in Deutschland – noch in Entwicklung sind und Angebote auf lokalen Märkten auch hier frühestens für 2021 erwartet werden.

4.2 Selektive Management-Interviews auf Ebene von Geschäfts- und Budgetverantwortlichen

In Interviews mit budgetverantwortlichen Managern der Unternehmensgruppe haben sich Datenschutz-Zertifizierungen als Anforderungen von Geschäftskunden als wichtigstes Bewertungskriterium herausgestellt. Auch aus der Online-Befragung hatte sich bereits ergeben, dass Vertriebsmitarbeiter bei der Geschäftsanbahnung vermehrt mit Kundenanforderungen über datenschutz-spezifische Zertifizierungen konfrontiert sind. Aber auch ohne konkrete Kundenanforderung sahen die Befragten in einer datenschutzspezifischen Zertifizierung das Potential für ein Alleinstellungsmerkmal, mit dem man sich von Mitbewerbern abzusetzen vermag, insbesondere zu jetziger Zeit als „early adopter", wenn sich der Zertifizierungsmarkt für ISO 27701 und Art. 42 DSGVO Zertifizierungen erst noch entwickelt. Zudem wurde mehr Transparenz über den heterogenen Zertifizierungsmarkt eingefordert, insbesondere im Zusammenhang mit Cloud-Service-Angeboten. Für eine international tätige Unternehmensgruppe sind darüber hinaus die unterschiedlichen Organisationsebenen im Unternehmen (Gruppe zentral, Segment zentral, Organisationseinheit dezentral) für Zertifizierungsinitiativen zu berücksichtigen.

5 Einordnung und Ausblick

Die unternehmensinternen Befragungen zeigen, dass eine Zunahme der Bedeutung und Geschäftsrelevanz datenschutzspezifischer Zertifizierungen im unternehmerischen Umfeld wahrgenommen wird. Dies korreliert mit den weiterhin bestehenden Unsicherheiten über die Anwendung und Einhaltung gesetzlicher Datenschutzanforderungen, insbesondere aus der DSGVO[11], denen man mittels einer Zertifizierung Herr zu werden versucht. Da sich der Markt datenschutz-spezifischer Zertifizierungen noch in Entwicklung befindet und relevante Zertifizierungsangebote nach Art. 42 DSGVO frühestens für 2021 erwartet werden, überrascht es nicht, dass der Kenntnisstand relevanter Interessengruppen über datenschutzspezifische Zertifizierungsangebote noch ausbaufähig ist. Es erscheint mithin zweckmäßig, den Markt für datenschutzspezifische Zertifizierungen weiter zu beobachten und neueste Erkenntnisse nach Analyse unternehmensweit zu kommunizieren. Für den Art. 42 DSGVO-Zertifizierungsmarkt wird es dabei besonders interessant, wie private Zertifizierungsstellen eine Balance zwischen einerseits abstrakten, übertragbaren und damit mehrfachverwertbaren und andererseits hinreichend konkreten und spezifischen Konformitätsbewertungsprogrammen für Produkte, Dienstleistungen und Prozesse erreichen werden.

Mit ersten ISO/IEC 27701-Pilotierungszertifizierungen suchen Geschäftsbereiche insbesondere im Umfeld von Unternehmensgeschäften (B2B-Markt) Vorteile als Erstanwender („early adopters") und damit Alleinstellungsmerkmale gegenüber Mitbewerbern auszutesten. Gerade für Zertifizierungsstandards der ISO-Familie bietet sich hierbei ein zentrales Zertifizierungsmanagement mit zentraler Budgetallokation zur Realisierung von Mengen- und Standardisierungsvorteilen an (z. B. über Dachzertifizierung und/oder Matrix-Zertifizierungsverfahren).

Als Ausblick lässt sich festhalten, dass gerade für multinationale Unternehmensgruppen mit unterschiedlichen Geschäftsfeldern ein modulares Umsetzungskonzept mit einer Kombination datenschutzspezifischer Zertifizierungen (z. B. ISO/IEC 27701 für Unternehmensgeschäfte – B2B und Art. 42 DSGVO für den Verbrauchermarkt – B2C) opportun erscheint, um Zertifizierungsvorteile auf unterschiedlichen Märkten und für unterschiedliche Interessengruppen bestmöglich zu realisieren.

10 Siehe oben unter Ziffer II 2).

11 Man denke nur zuletzt an die weitreichende rechtliche Unsicherheit für Drittstaatentransfers, die der EuGH aktuell durch das Schrems II-Urteil hinterlassen hat.