01.24

ZRFC

Risk, Fraud & Compliance

19. Jahrgang
Februar 2024
Seiten 1–48

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

ESV ERICH SCHMIDT VERLAG
100 Jahre

In Kooperation mit
DICO
Deutsches Institut für Compliance

64683

IDW PS 980 und Art. 42 DSGVO

Hat hier der deutsche Prüfungsstandard für Compliance-Management-Systeme eine Zukunft?

Dr. Christian Schefold*

Dr. Christian Schefold

Die Datenschutz-Grundverordnung1 (DS-GVO) sieht Datenschutz als Compliance-Management-System. Blickt man auf die Struktur der Verordnung, so enthält diese alle wesentlichen Elemente eines solchen. Da darf auch eine Zertifizierung eines Datenschutz-Compliance-Systems nicht fehlen. Art. 42 DSGVO befasst sich mit der Zertifizierung und Art. 43 DSGVO mit der Zulassung von Zertifizierern. Der entsprechende Erwägungsgrund Nr. 100 DSGVO hält sich äußerst kurz und bietet keine Interpretationshilfe. Zertifizierungsverfahren, Datenschutzsiegel und Datenschutzprüfzeichen benötigen eine Grundlage, idealerweise einen Standard. Dieser Bericht stellt die erste EU-weit anerkannte Prüfungsgrundlage von Europrivacy vor. Trotz der Unterstützung von Europrivacy durch die Europäische Kommission und den Europäischen Datenschutzausschuss fremdeln die allermeisten Datenaufsichtsbehörden in der Europäischen Union noch mit Datenschutzstandards, Zertifizierungen und der Zulassung von Zertifizierern. Sind Wirtschaftsprüfer und der Prüfungsstandards IDW PS 980 eine Lösung?

1 Einleitung

Seit dem 25 Mai 2018 gilt in der gesamten Europäischen Union, wie aber auch in den Staaten des Europäischen Wirtschaftsraumes, die DSGVO. Selbst in Großbritannien findet sie auch nach dem Austritt des Vereinigten Königreichs noch Anwendung. Die Schweiz hat sich ein eigenes, an der DSGVO orientiertes Schweizer Datenschutzgesetz (revDSG) gegeben, das unlängst am 1. September 2023 in Kraft getreten ist. Art. 13 revDSG sieht ebenfalls eine Zertifizierung für Hersteller von Datenverarbeitungssystemen oder Datenverarbeitungsprogrammen sowie der Verantwortlichen und Auftragsverarbeiter vor. Damit geht das Schweizer Recht trotz deutlich knapperem Gesetzeswortlaut mit dem Einbezug von System und Softwareherstellern über den Art. 42 DSGVO hinaus. Diese Erweiterung ist sinnvoll und pragmatisch, denn sie erlaubt den Verantwortlichen und Auftragsverarbeitern, die Zertifizierung der eigenen Datenverarbeitung auf bereits zertifizierte Systeme und Programme aufzubauen. Es ist zu hoffen, dass sich diese Lücke der DSGVO entgegen der bisherigen öffentlichen Anwendungspraxis pragmatisch durch die Verfasser von Zertifizierungsstandards und zukünftigen Zertifizierer wird schließen lassen. Bereits bestehenden und auch zukünftigen Datenschutzstandards — wie auch den darauf aufbauenden Zertifikaten und Prüfzeichen — steht mindestens ein großer europäischer und damit wahrscheinlich auch weltweiter Markt offen.

Nach Mitteilung der Europäischen Kommission[22] ist Europrivacy der erste Zertifizierungsmechanismus, mit dem die Einhaltung der DSGVO nachgewiesen wird. Die Genehmigung durch den Europäischen Datenschutzausschuss für dieses allererste Datenschutzsiegel liegt vor. Hinter Europrivacy steht das European Centre for Certification and Privacy in Luxemburg. Zugelassene Zertifizierer müssen die erforderlichen rechtlichen und technischen Kenntnisse vorweisen. Bei der Umsetzung der Anforderungen sollen zugelassene, sogenannte Implementoren helfen. Der Zertifizierungsvorgang muss die anwendbaren Grundsätze der Standards ISO/IEC 17065 und 17021-1 erfüllen. Die Entwicklung des Zertifizierungssystems von Europrivacy wurde sowohl von der Europäischen Kommission als auch der Schweiz gefördert. Auch wenn die Her-

* Dr. Christian Schefold, LL. M., ist Partner im Berliner Büro der globalen Wirtschaftskanzlei Dentons und Co-Head der deutschen Compliance Praxis. Seit 2011 kommentiert er in der ZRFC die Entwicklungen und Anwendungsbereiche des IDW PS 980 und anderer Standards.

1 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (in Kraft getreten am 25. Mai 2018).

2 Abrufbar unter https://digital-strategy.ec.europa.eu/de/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr (Stand: 21.12.2023).

steller von Datenverarbeitungssystemen und Datenverarbeitungsprogrammen noch nicht ausdrücklich im Scope des Zertifizierungssystems erfasst sind, besteht die Hoffnung, dass auch die Möglichkeiten des revDSG erfüllt werden und diese, für den Danteschutz bei der Verarbeitung in Unternehmen wesentlichen Grundlagenprodukte in die Zertifizierung einbezogen werden.

Das Institut der Wirtschaftsprüfer in Deutschland e. V. (Institut der Wirtschaftsprüfer — IDW) hat vor über zehn Jahren bahnbrechende Arbeit geleistet: In einer vielbeachteten internationalen Vergleichsarbeit wurden die damals wesentlichen Standards zum Aufbau von Compliance-Programmen — der Begriff eines Compliance Management Systems (CMS) bildete sich damals erst heraus — in der Welt verglichen und in einem neuen IDW-Prüfungsstandard Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen (IDW PS 980) zusammengetragen. Mittlerweile steht eine aktualisierte Neufassung gewissermaßen als zweite Auflage zur Verfügung.

2 Zertifizierung nach der DSGVO

Grundlage der Datenschutzzertifizierung sind die Art. 42 und 43 DSGVO. Art. 42 Abs. 1 DSGVO postuliert eine Förderpflicht der EU-Mitgliedstaaten, der Datenschutzaufsichtsbehörden, des Europäischen Datenschutzausschusses und auch der Europäischen Kommission für datenschutzspezifische Zertifizierungsverfahren sowie von Datenschutzsiegeln und Datenschutzprüfzeichen, die zum Nachweis dafür dienen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern auch eingehalten wird (Hersteller von Datenverarbeitungssystemen und Datenverarbeitungsprogrammen sind nicht genannt.). Da Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) gesondert angesprochen werden, muss eine Datenschutzzertifizierung nach EU-Maßstäben auch verhältnismäßig sein und die besonderen Datenverarbeitungssituationen der KMU berücksichtigen. Dies bietet möglicherweise auch eine Grundlage dafür, dass die Anforderungen der DSGVO gegenüber KMU mit Augenmaß gehandhabt werden sollten. Schließlich ist eine wesentliche Kritik an der DSGVO, dass diese — mit Ausnahme des privaten Bereichs der Familie — keine Ausnahmen in der Anwendung ihrer Anforderungen vorsieht. Die Zertifizierung selbst muss freiwillig geschehen und über ein transparentes Verfahren zugänglich sein (Art. 42 Abs. 3 DSGVO). Mit diesem Postulat stellt sich allerdings die Frage, ob eine Zertifizierung zur Grundvoraussetzung von Einkaufsbedingungen oder Ausschreibungen gemacht werden kann. Dies dürfte gerade ein Thema für Öffentliche Ausschreibungsverfahren sein. Zumindest als ein Auswahlkriterium sollte sie berücksichtigt werden können. Auch hat eine Zertifizierung keine Auswirkung auf die eigentlichen Datenschutzverpflichtungen und die Aufgaben und Befugnisse der Aufsichtsbehörden (Art. 42 Abs. 4 DSGVO). Das dürfte aber den Wert einer Zertifizierung nicht schmälern, wenn diese ordnungsgemäß erlangt ist. Zumindest stellt sie ein Indiz für eine verantwortungsvolle Datenverarbeitung durch die jeweiligen Verantwortlichen oder Auftragsverarbeiter dar. Schon allein die Arbeitsüberlastung bei den deutschen Aufsichtsbehörden könnte hier einen Vertrauensbonus herstellen, der die Arbeit der Behörden erleichtert. Allerdings stehen die 17 Aufsichtsbehörden Deutschlands der Zertifizierung insgesamt noch überwiegend skeptisch gegenüber.

Die DSGVO sieht in Art. 42 die Möglichkeit einer Zertifizierung vor.

Das Europäische Datenschutzsiegel gemäß Art. 42 Abs. 5 DSGVO kann nur aufgrund von Zertifizierungskriterien, die vom Europäischen Datenschutzausschuss genehmigt wurden, durch entsprechend Art. 43 DSGVO zugelassene Zertifizierungsstellen vergeben werden. Allerdings kann jede Datenschutzaufsichtsbehörde, dass heißt für Deutschland der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wie auch jeder der 16 Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI), Zertifizierungskriterien genehmigen. Allerdings ruft die DSGVO europaweit sowie das Bundesdatenschutzgesetz (BDSG) deutschlandweit zur Kohärenz aller Behörden auf. Dies dürfte den Wert des bereits europaweit durch den Europäischen Datenschutzausschuss genehmigten Europrivacy-Zertifizierungsverfahren deutlich erhöhen. Dem Wortlaut des Art. 42 DSGVO nach, können auch BfDI und LfDIs selbst zertifizieren. Sollte es für Deutschland keine zugelassenen Zertifizierungsstellen geben, kann sich aus der Förderpflicht der Zertifizierung nach Art. 42 Abs. 1 DSGVO möglicherweise eine Pflicht zur Zertifizierung durch BfDI oder LfDI ergeben, insbesondere dann, wenn es bereits ein EU-weit zugelassenes Zertifizierungssystem wie Europrivacy gibt.

Ein Zertifizierungsverfahren setzt Transparenz der Beteiligten voraus (Art. 42 Abs. 3 und 6 DSGVO). Ein Zertifikat hat eine Gültigkeitsdauer von drei Jahren (Art. 42 Abs. 7 DSGVO) und kann verlängert werden. Ein einmal bereits erteiltes Zertifikat hat aber keine Bestandsgarantie. Sollten die Anforderungen (insbesondere wohl wesentliche Anforderungen) entfallen, können sowohl der Zertifizierer als auch die zuständige Aufsichtsbehörde das Zertifikat entziehen. Damit besteht für BfDI und LfDI insbesondere bei Datenschutzverstößen eine weitere „Waffe“: der Entzug der Datenschutzzertifizierung. Diese Maßnahmen können insbesondere bei einem Reputationsaufbau über eine Zertifizierung massive Folgen für ein Unternehmen haben. Damit dürfte der Entzug auch nur bei erheblichen Verstößen, nach Androhung des Zertifikatsentzugs

und ausreichender Gelegenheit einer Selbstheilung beziehungsweise Nachbesserung oder Reparatur möglich sein.

Letztendlich will die Zertifizierung nach Art. 42 Abs. 2 in Verbindung mit Art. 46 Abs. 2 Buchst. f) DSGVO eine besondere Möglichkeit für Verantwortliche und Auftragsverarbeiter für personenbezogene Daten bieten, die außerhalb des räumlichen Geltungsbereichs der DSGVO liegen. Eine Zertifizierung — etwa nach den Europrivacy-Kriterien — kann als geeignete Garantie für den Transfer und die Verarbeitung personenbezogener Daten in Drittstaaten, die kein EU-adäquates Datenschutzniveau haben, gelten. Allerdings setzt die Zertifizierung für einen Garantiestatus nach Art. 46 DSGVO auch eine durchsetzbare Verpflichtung zur Anwendung der zertifizierten Garantien insbesondere für Betroffene voraus. Damit sind ein Abschluss und die Durchsetzbarkeit der EU-Standardvertragsklauseln nach wie vor erforderlich — und genügt aber für sich allein. So besteht eigentlich kein Bedarf für eine Art. 42 DSGVO-Zertifizierung für Verantwortliche und Auftragsverarbeiter in Drittstaaten. Auch in Bezug auf das EU-U.S. Data Privacy Framework, dem nach Safe Harbor und Privacy Shield dritten Versuch eines Angemessenheitsbeschlusses für den Austausch personenbezogener Daten mit den USA, dürfte eine Datenschutzzertifizierung außerhalb einer Reputationssteigerung keinen Vorteil bringen. Die Herausforderung des EU-U.S. Data Privacy Framework ist nach wie vor die Durchsetzbarkeit der Datenschutzregeln in den USA. Und hier bietet eine Zertifizierung allein keine Lösung.

Die Zertifizierung ist vom EDSA, dem BfDI und den LFDIs abhängig.

Die Zertifizierung nach Art. 42 DSGVO wird durch Zertifizierungsstellen gemäß Art. 43 DSGVO oder aber den Datenschutzaufsichtsbehörden selbst erteilt. Für die Zertifizierung selbst sind die Zertifizierungsstellen verantwortlich (Art. 43 Abs. 4 DSGVO). Eine Zertifizierung setzt die vorherige Unterrichtung der zuständigen Aufsichtsbehörden (also je nachdem dem der BfDI oder der LfDI des Sitzbundeslandes) durch den Zertifizierer voraus, einschließlich einer Begründung dafür (Art. 43 Abs. 5 DSGVO — Welches auch für einen Widerruf einer Zertifizierung gilt.). BfDI und LfDI können den Zertifizierer anweisen, eine Zertifizierung nicht zu erteilen oder diese zu widerrufen (Art. 43 Abs. 1 in Verbindung mit Art. 58 Abs. 2 DSGVO). Auch wenn dies nur eine Unterrichtungspflicht ist, ist diese Einschränkung der Zertifizierungstätigkeit wohl in Praxis eine Genehmigungsvorbehalt. Welcher Zertifizierer will es riskieren, dass die nach Unterrichtung innerhalb der wohl eher langfristigen Bearbeitungszeit des BfDI oder des zuständigen LfDI erteilte Zertifizierung dann widerrufen werden muss? Auch stellt sich die Frage, wer sich dann gegen die Anweisung der Behörde wehren kann — der Zertifizierer als unmittelbarer Normadressat oder der betroffene Verantwortliche beziehungsweise Auftragsverarbeiter? Diese Bestimmung dürfte sich insbesondere vor dem Hintergrund der kritischen Haltung deutscher Aufsichtsbehörden gegenüber der Zertifizierung als wesentliches Hindernis für den Erfolg einer Europrivacy-Zertifizierung in Deutschland darstellen.

Eine Zertifizierungsstelle muss über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, worüber als Aufsichtsbehörden wohl eher die LfDIs als der BfDI mangels konkreter Zuständigkeitszuschreibung im BDSG zu entscheiden haben. Grundsätzlich genügt dies für eine erforderliche Akkreditierung (Art. 43 Abs. 1 DSGVO). Formell tritt neben das Fachwissen noch eine Unabhängigkeit hinzu (Art. 43 Abs. 2 Buchst. a) DSGVO); sie müssen dem zuständigen LfDI nachweisen, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen (Art. 43 Abs. 2 Buchst. e) DSGVO). Damit dürfte wohl vor allem die Unabhängigkeit gegenüber Verantwortlichen und Auftragsverarbeiter gemeint sein. Berufsgruppen mit standesrechtlicher Unabhängigkeitsverpflichtung, wie etwa Rechtsanwälte und Wirtschaftsprüfer, dürften es hier einfacher haben als andere Berufsstände. Ob damit Verbände und andere Vereinigungen der IT-Industrie, die in Bezug auf Datenschutzverhaltensregeln nach Art. 40 DSGVO besonders angesprochen werden, als Zertifizierer überhaupt grundsätzlich infrage kommen, dürfte schwierig zu beantworten, aber nicht grundsätzlich unmöglich sein. Ferner muss ein Zertifizierer sich zur Zusammenarbeit mit den Datenschutzaufsichtsbehörden verpflichten (Art. 43 Abs. 2 Buchst. b) DSGVO) sowie die entsprechenden Verfahren für eine Zertifizierung, ihre Überprüfung, den Widerruf sowie den Umgang mit Beschwerden über eine Zertifizierung nachweisen (Art. 43 Abs. 2 Buchst. c) und d) DSGVO). Für Zertifizierungsstellen können weitere Anforderungen — ähnlich den Zertifizierungsanforderungen selbst — durch die Aufsichtsbehörden in demselben Verfahren aufgestellt werden (Art. 43 Abs. 3 und Abs. 6 DSGVO). Diese liegen bei Europrivacy ebenfalls vor.

Die Akkreditierung von Zertifizierungsstellen kann durch den zuständigen LfDI oder eine nationale Akkreditierungsstelle dann widerrufen werden, wenn die Voraussetzungen für eine Akkreditierung nicht mehr vorliegen oder aber die Zertifizierungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind (Art. 45 Abs. 7 DSGVO). Dies unterstreicht die Abhängigkeit der Zertifizierung und auch Zertifizierungsstellen von den Datenschutzaufsichtsbehörden. Fehlende oder ungenaue Unterrichtung, möglicherweise vorschnelle Zertifizierung während des Verwaltungsverfahrens nach Unterrichtung oder selbst Freiheiten in der Interpretation von Zertifizierungsanforderungen können zum Entzug der Akkreditierung führen. Es gilt zwar das Verhältnismäßigkeitsgebot, welches dann aber wohl erst

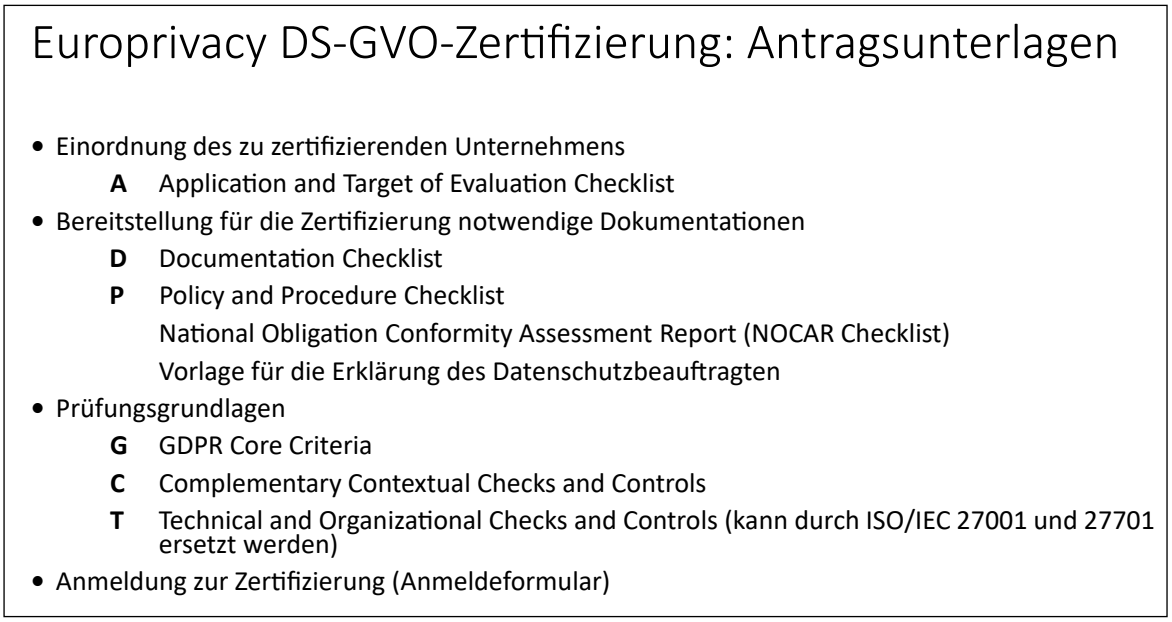

Abbildung 1: Europrivacy-Antragsunterlagen

mal gegen Versagungsentscheidungen gerichtlich zum Ansatz gebracht werden müsste. Art. 45 Abs. 7 DSGVO stellt ein scharfes Disziplinierungsschwert gegenüber den Zertifizierungsstellen dar: Kommt es zu einem Datenschutzvorfall bei einem zertifizierten Verantwortlichen oder Auftragsverarbeiter stellt dies wohl zugleich die Akkreditierungsfrage in Bezug auf die zuständige Zertifizierungsstelle. Diese Kopplung der Zertifizierungsstelle an die Aufsichtsbehörde führt auch zur Durchsetzung der datenschutzrechtlichen Interpretationsansichten der Behörden und stellt damit eine erhebliche Einschränkung des Wirtschaftshandelns zertifizierungswilliger Verantwortlicher und Auftragsverarbeiter dar.

3 Zertifizierungsgrundlagen von Europrivacy

Eine Anmerkung vorweg: Die Unterlagen von Europrivacy stehen nicht frei zur Verfügung, sondern sind urheberrechtlich geschützt sowie entgeltpflichtig. Es gibt unterschiedliche Informationslevel und Unterlagenpakete auf Anfrage zu entsprechenden Preisen. Weitere Informationen hält die Europrivacy Academy über ihre Kurse bereit.[3] Das Verfahren zur Vorbereitung der Zertifizierung ist in einzelne Schritte gegliedert und wird mit ausführlichen Checklisten begleitet. Diese unterstützen ebenfalls eine Implementierung der Anforderungen im Unternehmen. (Siehe Abbildung 1)

Nach dem Verständnis von Europrivacy gibt ihr Zertifizierungsansatz eine Methodologie vor, die es erlaubt, die Konformität von Verarbeitungsvorgängen sowie Datenschutz-CMS mit der DSGVO und anderen anwendbaren Datenschutzgesetzen (etwa dem BDSG) zu prüfen und zu zertifizieren. Der Ansatz von Europrivacy soll ISO/IEC 17065 und ISO/IEC 170211 entsprechend sowie auch mit Zertifizierungen nach ISO/IEC 27001 und 27701 kombiniert werden können. Dementsprechend sind Prüfungsgrundlagen und Prüfungsvorgehensweise thematisch und funktional gegliedert und nicht entsprechend den klassischen Elementen eines CMS. Grundlage von Europrivacy ist die Herangehensweise beim Qualitätsmanagement von ergebnisorientierten Unternehmensprozessen und weniger die Bewertung eines in das Unternehmen und seinen Prozessen integrierten CMS. Ein Datenschutz-CMS wird nicht im Zusammenspiel mit anderen Unternehmensfunktionen, sondern aus dem Blickwinkel der in der DSGVO bereits verankerten Elementen geprüft. Dies ist für das Verständnis des Ansatzes von Europrivacy entscheidend.

Europrivacy bietet die erste, anerkannte Datenschutz-zertifizierungs-grundlage an.

Der Ablauf und die einzelnen Schritte der Zertifizierung nach dem Konzept von Europrivacy sind Folgende: (siehe Abbildung 2).

Die Prüfungskriterien richten sich strikt nach der DSGVO und den dazu erfolgten Stellungnahmen des Europäischen Datenschutzausschusses. Um allen behördlichen Anforderungen entgegenzukommen, wird der strikteste Ansatz gefahren. So geht Europrivacy davon aus, dass alle Unternehmen, die eine Zertifizierung beantragen, einen Datenschutzbeauftragten ernannt haben. In den Prüfungskriterien wird dann unter anderem abgefragt, ob durch Unternehmensrichtlinien den Mit-

3 Derzeit (Stand: Dezember 2023) kann ein Einsteigerkurs bereits für 50,00 Euro gebucht werden. Für einen Kurs zum anerkannten Implementor sind schon 1.800 Euro zu zahlen, der Kurs zum Auditor kostet 2.400 Euro, abrufbar unter https://academy.europrivacy.com/courses_pricing/ (Stand: 21.12.2023).

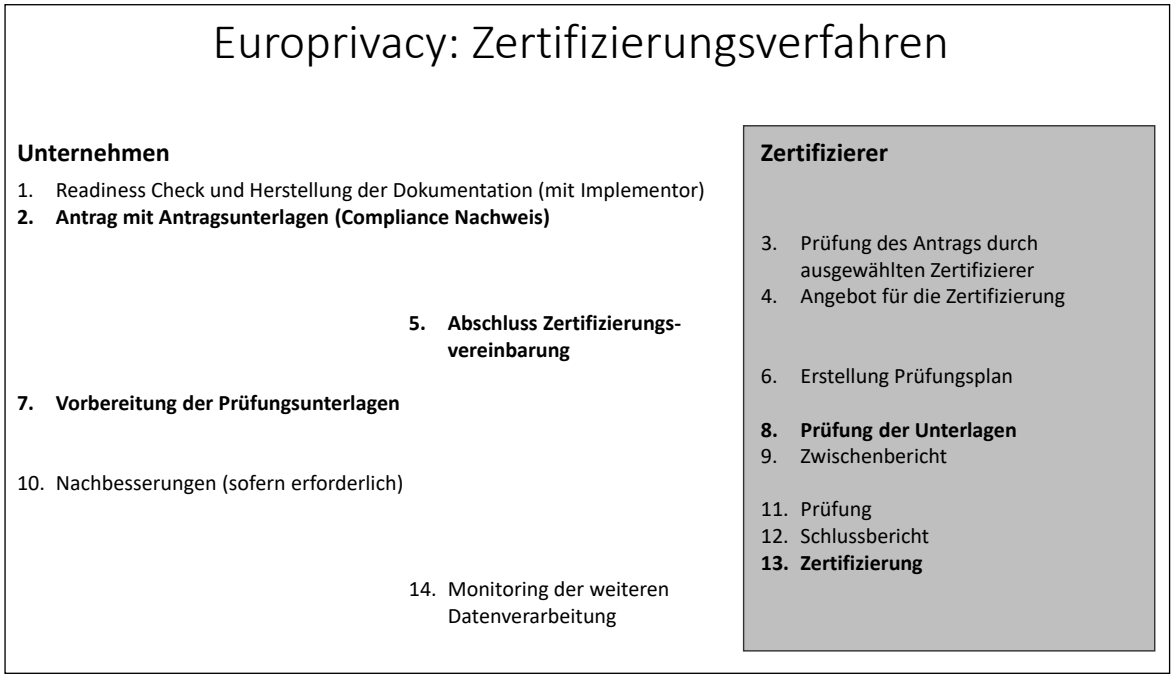

Abbildung 2: Europrivacy-Zertifizierungsverfahren

Es werden Verarbeitungen und Unternehmen nach Art. 42 DSGVO zertifiziert.

arbeitern des Unternehmens aufgegeben wird, dass der Datenschutzbeauftragte frühzeitig zu allen Datenschutzthemen involviert wird. Damit erhält der Datenschutzbeauftragte eine erheblich stärkere Stellung, als in der DSGVO eigentlich vorgesehen. Die Stellung entspricht eher dem Datenschutzbeauftragten nach dem Verständnis des alten BDSG mit Vorabkontrolle und weiteren Kontroll- und Eingriffsrechten. Gerade eine solche Funktion des Datenschutzbeauftragten wollten alle EU-Mitgliedstaaten mit Ausnahme Deutschlands nicht unterstützen.

Die Zertifizierungsgrundlagen von Europrivacy wurden aus einer akademischen Sicht entwickelt. Dem Standard steht ein Europrivacy International Board of Experts beratend zur Seite, dem zwar nicht nur Professoren, Institutsleiter und andere Akademiker, sondern auch Praktiker (zum Beispiel Rechtsanwälte) angehören. Gleichwohl ist der theoretische Hintergrund bei allen Dokumentationen zu den Zertifizierungsgrundlagen nicht zu übersehen. Es hat den Anschein, dass die Zertifizierung eine umfangreiche, selbst über die Anforderungen der DSGVO hinausgehende Dokumentation und auch Risikoabschätzung aller Datenverarbeitungsvorgänge voraussetzt.

Auch wenn das Ziel ist, die Datenverarbeitung eines gesamten Unternehmens zu zertifizieren, ist es nun auch möglich, den Zertifizierungsvorgang auf einzelne Datenverarbeitungen zu beschränken. Leider fehlt eine solche Möglichkeit für System- und Softwareprodukte. Es ist zu hoffen, dass diese Lücke nun nach dem Schweizer Modell geschlossen wird. Nach der Konzeption des Europrivacy-Standards ist es durchaus möglich.

Für jeden Mitgliedstaat sind Sonderbedingungen für die Zertifizierung in gesonderten Checklisten festgelegt. Dies betrifft für Deutschland die Regelungen des BDSG wie aber die Verlautbarungen des BfDI zu verpflichtenden Datenschutzfolgeabschätzungen. Zum BDSG werden die §§ 4, 26 und 31 BDSG sowie weitere Sonderregelungen für den öffentlichen Bereich hervorgehoben. Es überrascht, dass § 4 BDSG trotz der fehlenden Übereinstimmung mit der DSGVO trotzdem noch aufgeführt ist.

Nach Angaben von Europrivacy hat eine Europrivacy-Zertifizierung für Unternehmen eine Reihe von Vorteilen: Die Risikoanalyse als Checklisten-orientierte Vollständigkeitsprüfung ermöglicht es, rechtliche und finanzielle Risiken potenzieller DSGVO-Verstöße zu identifizieren und dagegen gezielt vorzugehen. Die DSGVO-Compliance-Prüfung erfolgt unabhängig durch einen sachkundigen Dritten. Insgesamt verschafft eine erfolgreiche Siegelerteilung eine Verbesserung der Reputation, der Stellung im Wettbewerb und eröffnet bessere Vermarktungschancen für Dienstleistungen. Kunden und Betroffene können Vertrauen aufbauen, und wenn zertifizierte Unternehmen auch in der Konstellation Verantwortlicher/Auftragsverarbeiter zusammenarbeiten, wird dies das Risiko von DSGVO-widrigem Verhalten sicherlich reduzieren. Ob sich ein Europrivacy-Siegel hinterher wirklich bezahlt macht, ist zu hoffen, muss sich aber noch in der Praxis beweisen. Es bestehen jedoch gute Chancen, dass sich durch ein solches Siegel der Marktwert erhöht und weitere Chancen auf ein nachhaltiges Wachstum ergeben.

Ein gutes Argument für Prüfung und Siegel, was von Europrivacy unverständlicher Weise selbst

nicht dargelegt wird, ist die Haftungsreduzierung für die Geschäftsleitung von Unternehmen. Die ordnungsgemäße Durchführung einer Prüfung nach dem Europrivacy-Konzept ist dazu geeignet, Defizite in der Anwendung der DSGVO im Unternehmen zu erkennen und abzustellen. Es ist aber eine Qualitätsmanagementprüfung, nicht jedoch eine Organisationsprüfung des Datenschutz-CMS. Hier sind weitere Prüfungsansätze — etwa nach IDW PS 980 — erforderlich.

Inwieweit der Eintritt in eine Europrivacy Community, die mit Teilnahme am Prüfungsprogramm und der Akademie verbunden ist, ein Wert an sich darstellt, wird sich zeigen müssen. Wenig plausibel ist es, dass ein Europrivacy-Siegel den internationalen Datentransfer verbessern soll. Da gibt es — wie zuvor beschrieben - weitere Voraussetzungen, die kaum in der Hand der betroffenen Unternehmen liegen.

Der umfassende, dabei eher theoretische Ansatz der Europrivacy-Zertifizierung führt zwangsläufig zu Überlegungen, ob nicht abgespeckte Zertifizierungen möglich sind. Gerade weil die Verfasser der DSGVO nicht so richtig an die Vorteile einer Zertifizierung glauben und eine erteilte Zertifizierung nicht mit entsprechenden Anscheinswirkungen etwa im Hinblick auf behördliche Verfahren versehen wollten. Eine Zertifizierung nach DSGVO-Maßstäben soll allenfalls eine Öffentlichkeitswirksamkeit haben, die aber das Vertrauen der Aufsichtsbehörden nicht so richtig genießt. Ziel der Zertifizierung ist nicht unbedingt der Verbraucher, sondern der Geschäftspartner, der gerne zur eigenen Absicherung zertifizierte Verarbeiter als Verantwortliche oder Auftragsverarbeiter einsetzt. Hier kann aber auch ein anderes Zertifizierungssystem eingesetzt werden, dass in Fachkreisen bereits Vertrauen genießt: die Prüfung eines Wirtschaftsprüfers nach dem Standard IDW PS 980.

4 Geeignetheit eines Vorgehens nach IDW PS 980

Der IDW PS 980 beschreibt ein Vorgehen für die Prüfung der Umsetzung von Compliance-Anforderungen, dass im Rahmen einer Standard-vergleichenden Methode entwickelt wurde. So entstanden, erlaubt dieser Prüfungsstandard eine universelle Anwendbarkeit für unterschiedlichste Compliance-Anforderungen, einschließlich denen der DSGVO. Ein entscheidender Vorteil des Prüfungsstandards IDW PS 980 ist hier gerade der Umstand, dass die Basis eines CMS und die Grundlagen seiner Prüfung nach wie vor zuerst festzulegen sind. Der IDW PS 980 lässt sich sehr einfach mit weiteren Standards und Zertifizierungsgrundlagen kombinieren und kann damit zu an die jeweiligen Anforderungen genau angepassten und praxisnahen Prüfungen und Prüfungsergebnissen führen.

Der Prüfungsstandard IDW PS 980 besitzt dabei eher eine Nähe zu den ISO/IEC-Werken 37001, 37002 und 37301. Die Vorgehensweise orientiert sich an Compliance-Management-Systemen und nicht am Qualitätsmanagement ergebnisorientierter Unternehmensprozesse.

4.1 Schritt 1: Definition der Prüfungsgrundlagen

Der große Vorteil des Prüfungsstandards IDW PS 980 ist seine Flexibilität und die damit verbundene Aufgabe, zunächst die Prüfungsgrundlagen zu definieren. Will man nicht selbst eigene Prüfungsgrundlagen entwickeln, kann auf die Vorarbeiten von Europrivacy zurückgegriffen werden. Da das Europrivacy-Konzept auf die Prüfung und Evaluation eines Datenschutzqualitätsmanagements ausgerichtet ist, muss dieses für eine Verwendung im Rahmen einer IDW-Prüfung angepasst werden. Dies ermöglicht auch, den vielbeschworenen Grundsatz der Verhältnismäßigkeit im Datenschutz Wirklichkeit werden zu lassen. Während im Qualitätsmanagement die hundertprozentige Befolgung der gesetzlich oder behördlich normierten Anforderungen das Maß aller Dinge ist, kann hier eine angepasste Compliance-Welt definiert werden, die auch Variablen in der Anwendung der DSGVO sowie Praxisnähe berücksichtigen kann. Eine IDW-Prüfung wird auf einen ganzheitlichen Compliance-Ansatz Wert legen und nicht allein punktuell sich auf die Erfordernisse der DSGVO ausrichten. (Siehe Abbildung 3)

Der Europrivacy Standard lässt sich auch als Grundlage für eine IDW PS 980 Prüfung nehmen; muss aber angepasst werden.

4.2 Schritt 2: Das CMS-Konzept

Entsprechend muss dann auch das CMS-Konzept gestaltet sein, soll die Prüfung nicht negativ verlaufen. Prüfungsansatz und Prüfungsobjekt sind voneinander abhängig und beeinflussen sich gegenseitig. Während bei der Zertifizierungsgrundlage von Europrivacy die DS-GVO als öffentlich-rechtliche Norm stets Geltungsvorrang hat und damit auch das nach diesen Anforderungen zu prüfende CMS-Konzept vollständig bestimmt, erlaubt der IDW PS 980 hier Interpretationen. Die DS-GVO stellt selbstverständlich Parameter für Prüfung und Konzept zur Verfügung, sowohl Prüfungsgrundlage als auch CMS-Konzept lassen aber Interpretationen und praktische Ausführungen der DS-GVO zu. Auch die Einbettung eines Datenschutz-CMS in das übrige CMS eines Unternehmens wie auch die Unternehmensorganisation als Ganzes kann bei der Anwendung des IDW PS 980-Standards definiert, konzeptioniert und damit Berücksichtigung finden. Hier ist der Ansatz von Europrivacy eingeschränkt.

4.3 Schritt 3: Die Prüfung

Auch die neue Auflage des IDW-Standards geht von einer Prüfung des CMS auf Angemessenheit und Implementierung als erste Prüfungsphase und

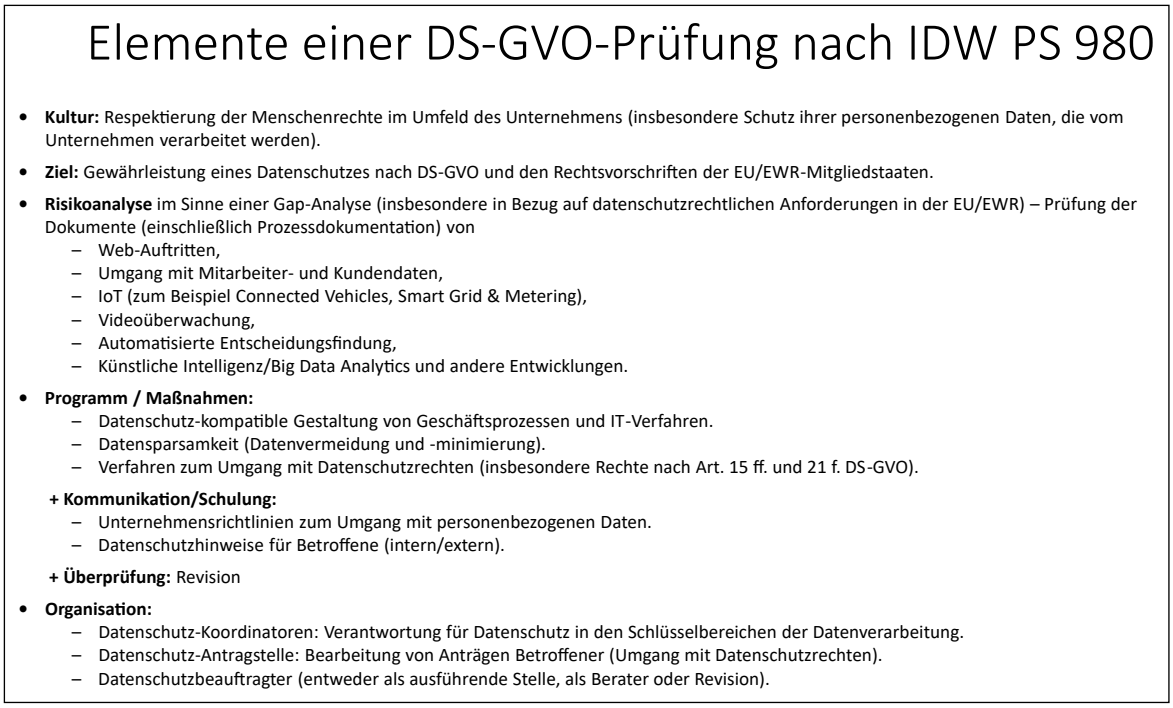

Abbildung 3: Elemente einer DS-GVO-Prüfung (IDW PS 980)

dann in einer abtrennbaren zweiten Phase von einer Wirksamkeitsprüfung aus. Diese zweite Phase kann dann zu einem späteren Zeitpunkt nachgeholt werden. Eine Prüfung kann sich auf eine Angemessenheitsprüfung beschränken, die zum einen (mit hinreichender Sicherheit) verifizieren soll, ob die in der CMS-Beschreibung benannten Regelungen zum unternehmensinternen Datenschutz (und damit die entsprechenden Maßnahmen) in Übereinstimmung mit den angewandten Grundsätzen zum Datenschutz in allen wesentlichen Belangen angemessen dargestellt sowie auch (abstrakt) geeignet sind, Risiken bei der Verarbeitung personenbezogener Daten zu erkennen, diese auch zu verhindern und — in einem weiteren Schritt — ob diese auch im Unternehmen umgesetzt wurden (Implementierung).

Für die Prüfung eines Datenschutz-CMS ist IDW PS 980 besser geeignet.

Die Wirksamkeitsprüfung beinhaltet in einem möglichen letzten Schritt die Angemessenheitsprüfung eines CMS und ergänzt diese um eine konkrete Geeignetheitsprüfung: Zum einen soll sich der Prüfer hinreichend sicher sein, dass die in der CMS-Beschreibung definierten Regelungen im Hinblick auf die jeweils angewandten CMS-Grundsätze (hier der Schutz der personenbezogenen Daten von Mitarbeitern, Kunden, Interessierten aber auch Mitarbeiter von Kunden und Interessierten) angemessen sind und auch umgesetzt wurden und dabei — zumindest im Prüfungszeitraum — im Wesentlichen (konkret) geeignet waren, Risiken für personenbezogene Daten wie etwa ungerechtfertigte Offenlegungen aber auch Störungen der Integrität von Daten rechtzeitig zu erkennen als auch zu verhindern.

5 Prüfung der Elemente eines CMS

Die Elemente Compliance-Kultur und Compliance-Ziele sind bei der Prüfung eines Datenschutz-CMS recht einfach zu bestimmen. Will man den Datenschutz in den Schutz der Persönlichkeitsrechte oder gar der Menschenrechte beziehungsweise der Business Human Rights einbetten (hier gibt es dann auch eine Verbindung zu einem LkSG-CMS), lässt sich damit ein großer Rahmen definieren beziehungsweise einen großen Bogen spannen. Zumindest ist keine grobe, erste Risikoanalyse erforderlich, um Ziele zu bestimmen und eine Kultur vorzugeben. Das bekannte Henne-Ei-Dilemma zwischen Zieldefinition und Ausrichtung der Risikoanalyse besteht hier nicht.

Die Risikoanalyse kann — wie etwa bei Europrivacy — eine Gap-Analyse sein. Sie kann sich aber auch auf die Effektivität und Effizienz der datenbezogenen Unternehmensabläufe in Bezug auf den Schutz personenbezogener Daten ausrichten. Ferner können die Verbindungen zu anderen Unternehmensabläufen getestet werden. So ist es möglich, zum Beispiel Verbindungen eines Produktentwicklungsprozesses zu Datenschutzentwicklungen zu ziehen. Gerade im Bereich neuer Technologien, etwa bei der Anwendung von Big Data oder künstlicher Intelligenz, ist hier eine frühzeitige Kopplung für den späteren Erfolg entscheidend.

Das Compliance-Programm (hier einschließlich der Elemente Kommunikation und Überwachung) beschränkt sich hier nicht unbedingt nur auf Anweisungen zum Umgang mit personenbe-

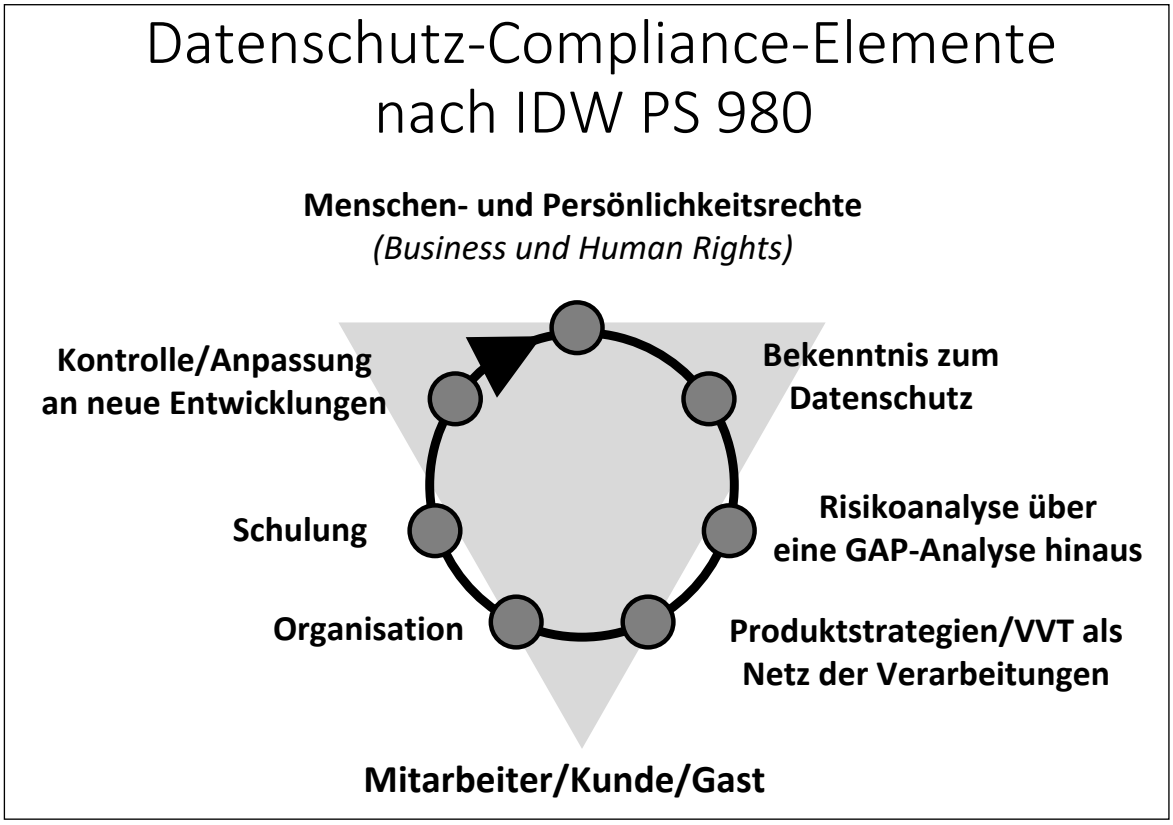

Abbildung 4: Datenschutz-Compliance-Elemente (IDW PS 980)

zogenen Daten oder Datenschutzhinweise wie auch Datenschutzfolgenabschätzungen, sondern sollte weitergehende Strategien, Leit- und Richtlinien umfassen. Es muss eine Durchdringung der Unternehmensabläufe mit einem Datenschutzverständnis erfolgen, um hier wirklich Datenschutzrisiken für die Zukunft auszuschließen. Risiken sind nicht allein Verstöße gegen die Anforderungen der DSGVO, sondern ein fehlendes Datenschutzbewusstsein bei Produktstrategien und auch übergeordneten Unternehmensabläufen. Es sind nicht nur Richtlinien und Hinweise zu prüfen sondern auch wie diese entstehen und weiterentwickelt werden, will man von einer Momentaufnahme absehen und eine konstante Datenschutz-Compliance erreichen. Besonderes Augenmerk muss auch die Organisation und Durchführung der Prozesse erhalten, die sich mit Anfragen und Anträgen von Betroffenen befassen. Hier sind sowohl Qualität der Behandlung solcher Anfragen und Anträge, aber auch die Effizienz bei der Bearbeitung im Unternehmen von hoher Bedeutung. Oft schließen gerade Auskunftsanträge nach Art. 15 DSGVO sehr viele Unternehmensbereiche mit ein. In dieser Hinsicht gewinnt auch das Verzeichnis für Verarbeitungstätigkeiten (Art. 30 DSGVO) eine besondere Kritikalität. Die DSGVO-Compliance dieses Verzeichnisses beschränkt sich nicht allein auf die Erfüllung der Mindestanforderungen nach der DSGVO, sondern umfasst auch seine Geeignetheit, in einem Auskunftsverfahren nach Art. 15 DSGVO als zentrale Auskunftsquelle über Verarbeitungen personenbezogener Daten einschließlich derer Verknüpfungen im Unternehmen. Es ist ein Vorteil eines Prüfungsansatzes nach IDW PS 980, wenn auch weitergehende, praxisnahe Anforderungen in eine Prüfung aufgenommen werden können und dafür gegebenenfalls weniger relevante Vorschriften eine geringere Aufmerksamkeit erhalten. Compliance-Überwachung und damit einhergehende Verbesserung stellen die kontinuierlichen Begleiter eines derartigen Programmansatzes dar – und sind in ihrer Verknüpfung mit den aktuell bestehenden Prozessen selbst Prüfungsgegenstand.

Eine Prüfung nach IDW PS 980 kann besser auf das Unternehmen angepasst werden und ist unabhängig von Datenschutz-Behörden.

5.1 Anforderungen an die Prüfer

Eine Prüfung ohne die erforderlichen und aktuellen Kenntnisse der Informationstechnologie sowie Medien aber auch der Cognitive Science (zu künstlicher Intelligenz) sowie Kybernetik und deren rechtliche Einordnung wird kaum möglich sein. Gerade bei einer Prüfung nach IDW PS 980 ist ein breiter Wissensrahmen verknüpft auch mit der Kenntnis von Unternehmensabläufen gerade in dem Spektrum der Neuen Technologien entscheidend. Während eine Checklisten-Prüfung nach den Zertifizierungsgrundlagen von Europrivacy zwar technische wie auch rechtliche Grundkenntnisse zur Datenverarbeitung und dem Datenschutz erfordert, geht die IDW-Prüfung darüber hinaus.

6 Verhältnismäßigkeit

Datenschutz ist Verwaltungsrecht, und Verwaltungsrecht wird vom Grundsatz der Verhältnismäßigkeit bestimmt. Der Datenschutz stellt besondere Anforderungen an Verarbeiter personenbezogener Daten (Verantwortliche im Besonderen aber auch Auftragsverarbeiter) dar, die durch die öffentliche Gewalt zum Schutz des Gemeinwesens aber auch des Einzelnen aufgestellt werden. Es sind Eingriffe in die Wirtschafts- und Handlungsfreiheit der Unternehmen, die sehr wohl abgewogen werden müssen. Diese Abwägung und ihre Umsetzung sind durch die Datenschutzaufsichtsbehörden zu prüfen. Dabei sind diese nicht allein der „Schutzengel" der Betroffenen, sondern müssen eine Interessenabwägung zwischen den Rechten des Einzelnen und den Geschäftschancen des Unternehmens treffen. Diese Abwägung ist vorher im Unternehmen vorzunehmen und ergibt die Strategie, die Leit- und Richtlinien im Umgang mit personenbezogenen Daten. Die Dokumentierung dieser Abwägung ist die Grundlage der Datenschutz-Compliance. Diese Abwägung muss den Grundsätzen der EU-Grundrechtscharta und der DSGVO entsprechen und dann über Einzelmaßnahmen im Unternehmen im Einzelfall umgesetzt werden. Verhältnismäßigkeit bedeutet auch, die Situation der Unternehmen zu berücksichtigen und diese nicht unnötig zu überfordern. Die Abwägung im Unternehmen ist Prüfungsgegenstand einer Compliance-Prüfung. Dabei ist die Flexibilität gegenüber der Prüfung auf der Grundlage vordefinierter Checklisten ein Vorteil des IDW-Prüfungsansatzes. Dabei können Checklisten eine Grundlage darstellen, der IDW-Ansatz erlaubt aber deren Anpassung auf die Unternehmenswirklichkeit.

Eine kombinierte Zertifizierung nach IDW PS 980 für das Datenschutz-CMS und Europrivacy für Verarbeitungen personenbezogener Daten ist zu empfehlen.

7 Ausblick

Die Stärke der Zertifizierungsgrundlage von Europrivacy ist die Darstellung der Anforderungen der DSGVO in der Interpretation der Europäischen Kommission, des Europäischen Datenschutzausschusses und der Vielzahl von Aufsichtsbehörden. Auch hier gibt der Prüfungskanon allein schon Sicherheit beim Aufbau eines Datenschutz-CMS. Es ist zu erwarten, dass weitere Verordnungen der EU im Aufbau und in der Methodik der DSGVO folgen werden. Dies gilt insbesondere für die Verordnung zur künstlichen Intelligenz.

Gerade bei diesen Neuentwicklungen sind jedoch flexiblere Herangehensweisen für Compliance-Prüfungen sinnvoll. Aus den gesetzlichen Grundlagen lassen sich Grundanforderungen herleiten. Hierzu sind die Vorarbeiten einer Europrivacy sehr hilfreich. Diese Grundanforderungen sind aber in Bezug auf die Umsetzung und Umsetzbarkeit im Unternehmen anzupassen und mit der Unternehmens- und Geschäftssituation ins Verhältnis zu setzen.

Ein großer Vorteil einer Prüfung durch einen Wirtschaftsprüfer ist hier die Unabhängigkeit auch von und gegenüber den Aufsichtsbehörden. Während eine Zertifizierung auf den Grundlagen von Europrivacy faktisch einer Genehmigung der zuständigen Aufsichtsbehörde bedarf, bei Zweifeln der Behörde wieder entzogen werden kann und letztendlich sogar die Stellung des Zertifizierers wie auch von Europrivacy gefährdet, ist der Wirtschaftsprüfer nur dann zur Verantwortung zu ziehen, wenn er die Prüfungsmaßstäbe nach IDW PS 980 in vorwerfbarer Weise missachtet hat. Insoweit ist zu einer Compliance-Prüfung nach dem IDW-Standard unter Hinzuziehung der Aufbauleistung von Europrivacy zu raten. Dabei kann eine Zertifizierung der Datenverarbeitungsvorgänge nach den Grundlagen von Europrivacy durchaus mit einbezogen werden.