

Irene Karper, Sönke Maseberg

# Zertifikat für Datenschutz-Management

Neben der Verschärfung der gesetzlichen Vorgaben und einer Erhöhung der Bußgelder wird seit Jahren ein Gütesiegel für Datenschutz gefordert, um dem nach wie vor bestehenden Umsetzungsdefizit entgegenzuwirken. Der vorliegende Beitrag schlägt ein Auditierungsverfahren vor, das auf die Zertifizierung eines „vorbildlichen“ Datenschutz-Managements zielt.

## 1 Einleitung

In das Ende 2009 novellierte Bundesdatenschutzgesetz (BDSG) ist das zuvor intensiv und zum Teil kontrovers diskutierte Bundesdatenschutzauditgesetz nicht aufgenommen worden. Damit gibt es noch immer kein bundesweit einheitliches Auditierungsverfahren für Datenschutz, obwohl – insbesondere nach den vielen Datenschutzskandalen – ein solches Audit dringend notwendig erscheint und für viele Unternehmen und öffentliche Stellen von Interesse ist. Denn ein Datenschutzaudit – freiwillig, von Experten durchgeführt und von einer unabhängigen Zertifizierungsstelle bescheinigt – stärkt das Vertrauen von Kunden bzw. Bürgern in die geprüfte und zertifizierte Institution.<sup>1</sup>

Mit diesem Beitrag soll die Diskussion um ein Datenschutzaudit neu belebt werden:<sup>2</sup> Er schlägt ein Auditierungs- und Zertifizierungsverfahren für ein Datenschutz-Management vor.

Zunächst wird in einem kurzen Überblick der Status Quo über die bereits bestehenden datenschutzrechtlichen Auditierungen und Zertifikate und deren Ausrichtung dargestellt. Anschließend wird erläutert, wofür das Zertifikat für Datenschutz-Management stehen soll, was ein Datenschutz-Management ist und wie ein solches Management zur Realisierung eines „vorbildlichen“<sup>3</sup> Datenschutzes aufgebaut sein muss, bevor anschließend der von den Autoren vorgeschlagene Auditierungs- und Zertifizierungsprozess beschrieben wird.

zudem einem „besonderen Gesetz“<sup>4</sup> vorbehalten, das trotz mehrerer Anläufe des Gesetzgebers bislang nicht existiert. Zuletzt wurde 2009 ein Entwurf eines Gesetzes zur Regelung des Datenschutzaudits<sup>5</sup> diskutiert, allerdings nicht vom Gesetzgeber verabschiedet, so dass der „verwaiste“ § 9a nach wie vor ohne nähere Bestimmungen bleibt.

Neben dem BDSG gibt es einige Landesdatenschutzgesetze, in denen Datenschutzaudits verankert sind. Als ein prominentes Beispiel sei hier § 43 Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H) genannt, welches ein Auditverfahren im behördlichen Umfeld für Datenschutzkonzepte vorsieht, sowie § 2 LDSG S-H i.V.m. einer Gütesiegelverordnung, welcher ein Datenschutz-Gütesiegel für IT-Produkte statuiert.<sup>6</sup>

Beide Datenschutzaudits erfreuen sich seit einigen Jahren wachsender Beliebtheit und sind auch über die Landesgrenzen hinaus anerkannt. Der Ansatz des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) für ein Datenschutzaudit ist inzwischen auch auf europäischer Ebene mit dem Datenschutz-Gütesiegel „EuroPrise“ für IT-Produkte und IT-Services erfolgreich etabliert.<sup>7</sup>

Daneben normieren Standards der Informationssicherheit das Thema Datenschutz, wodurch auch datenschutzrechtliche Aspekte bei der Prüfung und Bewertung von Informationssicherheits-Managementsystemen und IT-Produkten

## 2 Status Quo

### 2.1 Rechtliche Grundlagen

Das BDSG enthält bereits seit dem Jahr 2001 in § 9a Anforderungen an ein Datenschutzaudit, welches allerdings die Prüfung von Datenverarbeitungssystemen und -programmen zum Gegenstand hat, nicht aber umfassend auf ein Datenschutz-Management ausgerichtet ist. Die nähere Ausführung dieses Datenschutzaudits ist

<sup>2</sup> Siehe auch die früheren Beiträge von Petri, DuD 2001, S. 150 ff.; Hladjk, DuD 2002, S. 672 ff.; Rösser, DuD 2003, S. 401 ff.; Voßbein, DuD 2004, S. 92 ff.; Schläger, DuD 2004, S. 459, 461; Hammer/Schuler, DuD 2007, S. 77 ff.

<sup>3</sup> Die Vorbildlichkeit eines Datenschutz-Managements ist notwendig, um einen Mehrwert gegenüber nicht-zertifizierten Institutionen zu erzielen, die sich „lediglich“ rechtskonform verhalten. Zu diesem Ansatz siehe auch Hammer/Schuler, DuD 2007, S. 77, 81.

<sup>4</sup> BGBl. I S. 904, 2002 I S. 2252.

<sup>5</sup> BT-Drs. 16/12011 vom 18.02.2009.

<sup>6</sup> Weitere Informationen hierzu sind unter [https://www.datenschutzzentrum.de/guetesiegel/infos\\_hersteller.htm#guetesiegelverordnung](https://www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm#guetesiegelverordnung) abrufbar (Stand: 04/2010).

<sup>7</sup> Siehe <https://www.european-privacy-seal.eu/> (Stand: 04/2010).



**Dr. Irene Karper**  
LL.M.Eur.

Zertifizierungsstelle  
datenschutz cert  
GmbH

E-Mail: [ikarper@datenschutz-cert.de](mailto:ikarper@datenschutz-cert.de)



**Dr. Sönke Maseberg**

Geschäftsführer  
datenschutz cert  
GmbH

E-Mail: [smaseberg@datenschutz-cert.de](mailto:smaseberg@datenschutz-cert.de)

<sup>1</sup> Zu diesen und weiteren Vorteilen eines Datenschutz-Zertifikats siehe auch Hammer/Schuler, DuD 2007, S. 77 ff.

und -Systemen Berücksichtigung finden. Hierzu seien bei Managementsystemen die Anforderungen von ISO 27001<sup>8</sup> für Informationssicherheits-Management-systeme (ISMS) und IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie bei Produkten die Anforderungen der Common Criteria genannt.

Gleichwohl ist festzustellen, dass diese Standards die Informationssicherheit fokussieren und damit zwar viele Aspekte zum Managementsystem sowie zu den technisch-organisatorischen Datenschutzmaßnahmen des § 9 i.V.m. Anlage BDSG erfassen, aber eben nicht alle Anforderungen des Datenschutzrechts abdecken. Der IT-Grundschutz-Baustein „Datenschutz“<sup>9</sup> reicht nicht aus, da er nicht zertifizierungsrelevant ist und nicht vollständig in den ISMS-Prozess integriert ist.

## 2.2 Handlungsbedarf

§ 9a BDSG nennt zwei Zielgruppen:

- „Anbieter von Datenverarbeitungssystemen und -programmen“ und
  - „datenverarbeitende Stellen“
- sowie zwei Untersuchungsgegenstände:
- Datenschutzkonzepte sowie
  - technischen Einrichtungen.

Aus unserer Sicht ist die datenschutzrechtliche Prüfung und Bewertung von IT-Produkten und -Systemen durch die vorhandenen Regelwerke ULD-Datenschutz-Gütesiegel, EuroPrise und Common Criteria hinreichend bewährt und abgedeckt. Handlungsbedarf sehen wir allerdings bei Datenschutzkonzepten bei datenverarbeitenden Stellen und deren Umsetzung. Denn hier bleibt insgesamt festzuhalten, dass ein bundesweit akzeptierter Standard für die Prüfung und Bewertung von Datenschutzaspekten in Unternehmen und Behörden fehlt.

Für diese Institutionen ist ein Zertifikat zum Datenschutz-Management sinnvoll.<sup>10</sup> Dazu muss das Rad nicht neu erfunden werden. Vielmehr bedarf es einer sinnvollen Zusammenführung bereits vorhandener Ansätze. Nachfolgend soll ein solches Auditierungs- und Zertifizierungssche-

ma dargestellt werden. Die Anforderungen orientieren sich dabei am Aufbau herkömmlicher Management-Auditierungen, fokussieren aber zugleich auf die Anforderungen des § 9a BDSG.

## 3 Zertifikat für Datenschutz-Management

Ziel des Zertifikats für Datenschutz-Management ist es, Unternehmen und Behörden die Möglichkeit zu geben, das Thema Datenschutz pro-aktiv und positiv zu besetzen, und dies durch ein Zertifikat nach außen hin zu dokumentieren.

Zertifiziert wird eine Institution – also eine datenverarbeitende Stelle – dahingehend, ob ein vorbildlicher Datenschutz etabliert und umgesetzt wird und ob die einschlägigen datenschutzrechtlichen Anforderungen erfüllt sind. Der Anwendungsbereich ist dabei einschränkbar auf einen klar abgegrenzten Bereich signifikanter Größe und mit hinreichender datenschutzrechtlicher Relevanz, wodurch auch Verfahren und Prozesse durch dieses Zertifikat erfasst werden können.

Die Grundidee zur Realisierung eines vorbildlichen Datenschutzes ist dabei, Datenschutz in der Institution nachhaltig zu etablieren und die Umsetzung kontinuierlich aufrecht zu erhalten – kurz gesagt, ein Datenschutz-Management zu betreiben. Dieses Datenschutz-Management wird typischerweise in einem Datenschutzkonzept dokumentiert, was im Rahmen der Auditierung und Zertifizierung neben der Umsetzung begutachtet wird.

## 4 Datenschutz-Management

Ein Datenschutz-Management sorgt für die Etablierung und nachhaltige Umsetzung der datenschutzrechtlichen Anforderungen in einer Institution. Es umfasst alle Regelungen, die für die Steuerung und Lenkung eines vorbildlichen Datenschutzes relevant sind.

Grob orientiert sich ein solches Management an der für Managementsysteme üblichen Vorgehensweise in Form eines PDCA (Plan-Do-Check-Act)-Zyklus, wie er etwa in den internationalen Normen ISO 27001 oder ISO 9000 etabliert ist. Es enthält zudem eine strukturierte Herangehensweise, um zunächst alle relevanten Anforderungen zusammenzustellen und diese anschließend umzusetzen.

## 4.1 Planung

Das Datenschutz-Management muss etabliert werden – insbesondere in Form eines ggf. gesetzlich vorgesehenen betrieblichen bzw. behördlichen Datenschutzbeauftragten oder einer gleichwertigen Institution (nachfolgend zusammenfassend als Beauftragter für Datenschutz bezeichnet) sowie entsprechender Managementstrukturen, damit ein vorbildlicher Datenschutz überhaupt realisiert werden kann. Datenschutz ist dabei als integraler Bestandteil der zu zertifizierenden Institution zu verstehen. Insofern müssen Datenschutzziele dokumentiert werden. Ferner muss die Datenschutz-Organisation so gestaltet werden, dass diese Ziele erfüllt werden können.<sup>11</sup>

Anschließend erfolgt eine Ist-Aufnahme mit Identifikation und Darstellung des Untersuchungsgegenstands und der einschlägigen gesetzlichen Rahmenbedingungen; erfasst werden dabei die Bereiche, die zum Untersuchungsgegenstand gehören, sowie alle relevanten Verfahren, Standorte, Gebäude, Systeme etc. (Zielobjekte).

Aus den direkt einschlägigen Gesetzen und Verordnungen werden anschließend Anforderungen abgeleitet und den Zielobjekten – soweit sinnvoll – zugeordnet, so dass sich Möglichkeiten bieten, Einzelaspekte zu gruppieren, Redundanzen aufzulösen oder spezielle Aspekte zu verdeutlichen. In diesem Kontext werden auch spezielle Datenschutzaspekte thematisiert: Vertraulichkeit, Anonymität, Transparenz, etc.

Abschließend wird daraus ein konkreter Anforderungskatalog erstellt, der als Vorgabe dient. Damit orientiert sich die Vorgehensweise an anderen Kriterienwerken zur Prüfung und Bewertung von Sicherheitseigenschaften.

Zur Aufstellung eines Anforderungskatalogs können sogenannte Datenschutzprofile verwendet werden. Diese stellen quasi einen Baukasten von Anforderungen zu verschiedenen Themenkomplexen dar, aus dem – abhängig vom konkreten Untersuchungsgegenstand – relevante Aspekte in den Anforderungskatalog aufgenommen werden können, die damit den für den jeweiligen Untersuchungsgegenstand anwendbaren Prüfmaßstab darstellen.

<sup>11</sup> Vgl. Hierzu auch Hammer/Schuler, DuD 2007, S. 77, 79.

<sup>8</sup> ISO/IEC 27001: 2005, Information technology – Security techniques – Information security management systems requirements specification.

<sup>9</sup> Vgl. zum IT-Grundschutz-Baustein „Datenschutz“ Simon, DuD 2007, S. 87 ff. sowie Meints, DuD 2006, S. 13 ff.

<sup>10</sup> Vgl. Hammer/Schuler, DuD 2007, S. 77 ff.; Hladjik, DuD 2002, S. 672 ff.; für Produkt-Audits siehe auch Petri, DuD 2001, S. 150 ff.

Um diesen Anforderungskatalog möglichst effizient und effektiv sowie möglichst vollständig aufstellen zu können – und um nicht noch einmal das „Rad neu zu erfinden“ –, werden weitestmöglich anerkannte und etablierte Kriterienwerke genutzt; in diesem Kontext die internationalen Normen ISO 27001 und ISO 27002<sup>12</sup>, die einen umfangreichen Erfahrungsschatz an wichtigen Aspekten zur Informationssicherheit enthalten. Als Alternative zu den Controls und Control Objectives aus ISO 27001/27002 ist auch eine Nutzung von Bausteinen und einzelnen Maßnahmen aus den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) möglich.

Die folgenden Datenschutzprofile sind derzeit verfügbar:

- D.1 Datenschutz-Management
- D.2 Rechtliche Zulässigkeit
- D.3 Datenschutz-rechtliche Prinzipien
- D.4 Mitarbeiter
- D.5 Physikalische Sicherheit
- D.6 IT-Infrastruktur
- D.7 Verfahren
- D.8 Penetrationstest

Die Datenschutzprofile sind bewusst nicht in Schichten angeordnet und beleuchten verschiedene Bereiche, wobei die meisten Datenschutzprofile stets anzuwenden sind. In Abschnitt 5 werden die Datenschutzprofile näher dargestellt.

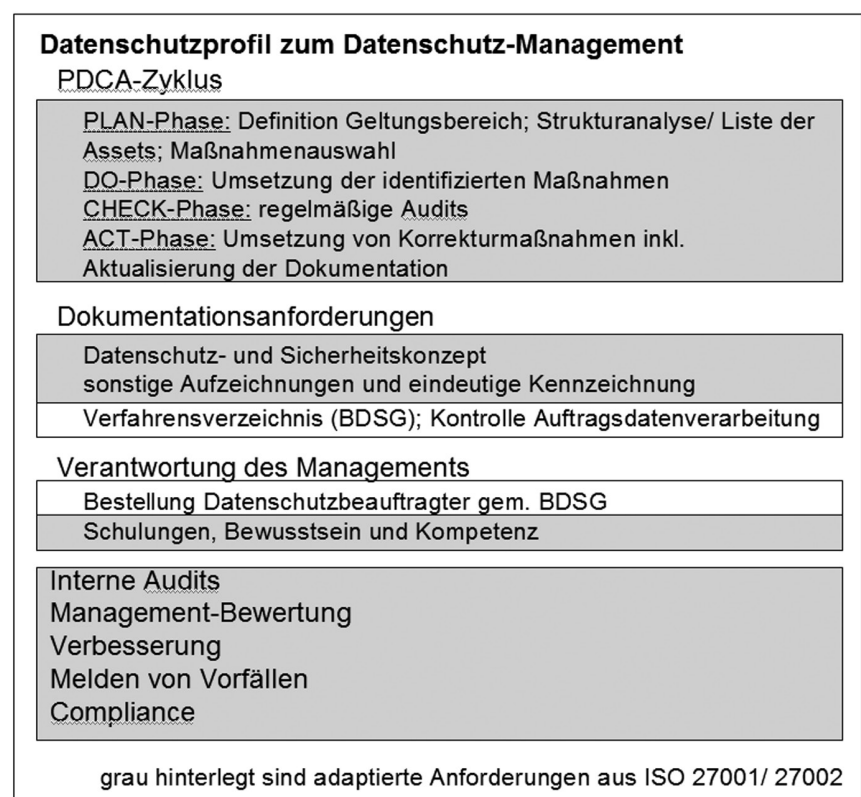
Die Auflistung der Datenschutzprofile ist nicht vollständig, d. h. es kann – auch in der Zukunft – konkrete rechtliche Anforderungen geben, für die die vorliegenden Datenschutzprofile unzureichend sind. Die Datenschutzprofile sind daher fortzuschreiben und an die aktuellen rechtlichen und technischen Anforderungen des BDSG sowie landesgesetzlicher und spezialgesetzlicher Regelungen zum Datenschutz anzupassen.<sup>13</sup>

Dieses Modell stellt eine strukturierte Herangehensweise dar, um die relevanten Einzelanforderungen zusammenstellen zu können, deren Umsetzung für die Erfüllung der zuvor abgeleiteten Anforderungen notwendig ist.

<sup>12</sup> ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management.

<sup>13</sup> Siehe zu den Beispielen für Datenschutzprofile sogleich Abschnitt 5.

Abbildung 1 |



## 4.2 Umsetzung und Dokumentation

Im Rahmen dieser „Do“-Phase erfolgt die Umsetzung der Anforderungen, die im zuvor definierten Anforderungskatalog aus den relevanten Datenschutzprofilen zusammengestellt wurden.

Wie die relevanten Aspekte des Anforderungskatalogs erfüllt werden, wird entsprechend von der zu auditierenden Institution dokumentiert, z. B. im

- Verfahrensverzeichnis;
- Datenschutzkonzept;
- Sicherheitskonzept.

Zudem wird die Zuordnung zur Erfüllung des Anforderungskatalogs z. B. im Rahmen eines internen Audits dokumentiert, so dass zu allen Aspekten des Anforderungskatalogs eine Erläuterung verfügbar ist.

Sofern sich eine Überschneidung zu anderen Regelwerken – etwa ISO 27001 oder IT-Grundschutz – ergibt, evtl. sogar mit Zertifikat versehen, kann auf die entsprechenden Dokumente Bezug genommen werden.

## 4.3 Regelmäßige Checks

Der Beauftragte für Datenschutz prüft die Umsetzung durch regelmäßige Kontrollen und interne Audits:

- Detektion von Vorfällen im laufenden Betrieb;
- Überprüfung der Einhaltung der Vorgaben;
- Überprüfung der Eignung und Wirksamkeit der Maßnahmen.

Die regelmäßigen Checks gehen über die gesetzlichen Anforderungen des BDSG hinaus; gleichwohl erfüllt der Beauftragte für Datenschutz damit zugleich seine Aufgabe zur Überwachung der Ordnungsmäßigkeit der Datenverarbeitung (§ 4g Abs. 1 BDSG) einschließlich der technisch-organisatorischen Sicherheitsmaßnahmen im Sinne der §§ 4f, 4g Abs. 1 Nr. 1, 9 BDSG.<sup>14</sup>

## 4.4 Kontinuierliche Verbesserung

In der „Act“-Phase werden Defizite oder Verbesserungsmöglichkeiten, die im Rahmen der Checks auffallen, im Rahmen

<sup>14</sup> Bzw. der entsprechenden landesgesetzlichen Normen.

dieses Prozesses zum Datenschutz-Management behoben und daraus folgende Maßnahmen und Ergebnisse geeignet dokumentiert.

## 5 Datenschutzprofile

Die derzeit verfügbaren Datenschutzprofile thematisieren unterschiedliche Anforderungen, die sich aus den einschlägigen rechtlichen Rahmenbedingungen und den spezifischen Datenschutzaspekten ergeben.

In diesem Abschnitt werden die Inhalte der Datenschutzprofile kurz vorgestellt.

### 5.1 Datenschutz-Management (D.1)

Das Datenschutzprofil „Datenschutz-Management“ thematisiert übergreifende organisatorische Aspekte des Datenschutzes. Der Begriff „Datenschutz-Management“ wird im IT-Grundschutz-Baustein B 1.5 „Datenschutz“ wie folgt definiert: „Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.“

Der Prozessansatz eines Datenschutz-Managements wird bei den internationalen Normen ISO 9001 oder ISO 27001 in Form des bereits erläuterten „PDCA-Zyklus“ definiert, in dem die Phasen Plan, Do, Check und Act einen Kreislauf bilden.

Aus dem PDCA-Zyklus' ergeben sich laut ISO 27001 die folgenden relevanten, z. T. auf Datenschutzbelange adaptierbaren Anforderungen:

- Dokumentationsanforderungen;
- Verantwortung des Managements;
- interne Audits;
- Management-Bewertung;
- Verbesserung;
- Melden von Vorfällen;
- Compliance.

Abb. 1 illustriert zu diesen Anforderungen, inwiefern auf Aspekte der ISO 27001 und ISO 27002 zurückgegriffen werden kann und welche Anforderungen in Form dieser Datenschutzprofile neu aufgenommen werden.

Wie der Graphik zu entnehmen ist, kann bezüglich des PDCA-Zyklus' weitgehend auf die ISO-Norm Bezug genommen werden. Demgegenüber sind Einzelanfor-

derungen aus dem BDSG in der ISO 27001 nicht explizit enthalten. Sie müssen also in diesem Datenschutzprofil vorgegeben werden – beispielweise zum Verfahrensverzeichnis und zum betrieblichen bzw. behördlichen Datenschutzbeauftragten. Danach muss das Verfahrensverzeichnis etwa die Anforderungen des § 4g Abs. 2 Satz 1 BDSG i.V.m. § 4e BDSG (oder einer entsprechenden landesgesetzlichen Norm des Datenschutzes) erfüllen.

Die Bestellungsvoraussetzungen eines betrieblichen bzw. behördlichen Datenschutzbeauftragten müssen umgesetzt sein. Dieser muss vertrauensvoll mit allen Beteiligten (Unternehmensführung, Mitarbeiter, unternehmensinterne Organe wie z. B. Betriebsrat, QM-Beauftragte, IT-Sicherheitsbeauftragter und Aufsichtsbehörden) zusammenwirken und in relevante Prozesse (z. B. Einführung neuer Software, Entwurf von Richtlinien, Betriebsvereinbarungen, Verträgen, Auswertungen von Mitarbeiterdaten) eingebunden sein.

Beschwerden zum Datenschutz müssen im Rahmen eines „Beschwerde-Managements“ im Sinne der Rechte der Betroffenen vertraulich empfangen und bearbeitet werden können. Bei Einführung neuer Prozesse und Verfahren müssen Prüfprozesse für eine Vorabkontrolle integriert sein; Vorabkontrollen müssen dokumentiert werden.

### 5.2 Rechtliche Zulässigkeit (D.2)

Das Datenschutzprofil „Rechtliche Zulässigkeit“ thematisiert den zentralen Aspekt der rechtlichen Zulässigkeit einer Datenverarbeitung personenbezogener Daten.

Zwei Beispiele: Falls Auftragsdatenverarbeitung Teil des Anwendungsbereiches ist, sind dementsprechend die Anforderungen aus § 11 BDSG zu berücksichtigen. Oder falls eine mobile Datenverarbeitung von unterwegs aus genutzt wird, ist zu prüfen, ob eine Datenverarbeitung personenbezogener Daten von Unterwegs aus zulässig ist.

### 5.3 Datenschutzrechtliche Prinzipien (D.3)

Für alle Verfahren, in denen personenbezogene Daten verarbeitet werden, sind die datenschutzrechtlichen Prinzipien zu prüfen und zu bewerten, z. B. Transpa-

renz, Datenvermeidung und -sparsamkeit, Pseudonymität, Anonymität, etc.

### 5.4 Mitarbeiter (D.4)

Zum Datenschutzprofil „Mitarbeiter“ gehören die Sensibilisierung von Mitarbeitern sowie die Verpflichtung auf das Datengeheimnis.

### 5.5 Physikalische Sicherheit (D.5)

Das Datenschutzprofil „Physikalische Sicherheit“ thematisiert die Sicherheit von Gebäuden und Räumen, in denen Einrichtungen und Systeme untergebracht werden, um personenbezogene Daten zu verarbeiten.

Hierbei bietet sich die Möglichkeit, auf etablierte Standards zur Zutrittskontrolle (Control A.9.1.2 in ISO 27002) und zur sicheren Entsorgung (Control A.9.2.6 in ISO 27002) zu verweisen.

### 5.6 IT-Infrastruktur (D.6)

Das Datenschutzprofil „IT-Infrastruktur“ thematisiert die virtuelle Sicherheit von Systemen, mit denen personenbezogene Daten verarbeitet werden.

Auch hier bietet sich die Möglichkeit, auf etablierte Standards zurückzugreifen, um Anforderungen zu prüfen und zu bewerten – beispielweise zum Betriebs- und Kommunikationsmanagement, zum Änderungsmanagement, zu Zugangskontrollen oder zum Backup.

### 5.7 Verfahren (D.7)

Die Verarbeitung personenbezogener Daten auf Anwendungsebene wird in diesem Datenschutzprofil thematisiert, beispielsweise die Zugriffskontrolle oder das Rollen-/Berechtigungskonzept.

### 5.8 Penetrationstest (D.8)

Nicht zwingend anwendbar ist das Datenschutzprofil zum Penetrationstest, welcher allerdings sinnvoll angewendet werden kann, wenn ergänzende Tests durchgeführt werden sollen, um die Umsetzung von Regelungen und Vorgaben zu prüfen, z. B. zur Rechtevergabe.

## 6 Auditierungs- und Zertifizierungsprozess

Eine Zertifizierung des Datenschutz-Managements setzt die Einführung und Etablierung eines Datenschutz-Managements in der Institution voraus, so dass eine Prüfung der Umsetzung in Form eines Datenschutzaudits durch einen Auditor durchgeführt werden kann.

Das Zertifikat – mit dem der Institution ein „vorbildlicher Datenschutz“ attestiert wird – wird von einer Zertifizierungsstelle erteilt, die auch die Lizenzierung der Auditoren vornimmt.

### 6.1 Datenschutzaudit

Gemäß der Grundidee, einen Prozess zum Datenschutz zu etablieren, prüft der Auditor bei der Institution das Datenschutz-Management auf höherer „Meta“-Ebene. In diesem Zusammenhang wird der Auditor insbesondere begutachten, ob Datenschutz in der Institution integral verankert ist und eine strukturierte Herangehensweise angewendet wurde, um aus den gesetzlichen Anforderungen in Bezug auf den konkreten Untersuchungsgegenstand alle relevanten Anforderungen zu erfassen. Neben der Begutachtung des Prozesses werden auch Einzelaspekte der Umsetzung überprüft.

Die Prüfung und Bewertung erfolgt in den drei Phasen Vorbereitung, Pre-Audit und Audit. Das Datenschutzaudit umfasst alle bestehenden Prozesse des Datenschutz-Managements. Die Bewertung berücksichtigt, ob Maßnahmen getroffen werden, die über das gesetzlich geforderte Maß hinausgehen (diese werden als vorbildlich bewertet), ob „angemessene/adäquate“ oder „gesetzeskonforme“ Maßnahmen ergriffen oder nicht umgesetzt werden.

Es wird erwartet, dass der Auditor die folgenden Punkte durchführt und dokumentiert:

- Prüfung auf Plausibilität, Nachvollziehbarkeit und Vollständigkeit der strukturierten Herangehensweise;
- Bewertung der Ableitung aus den einschlägigen Gesetzen und Verordnungen auf die Anforderungen samt Bezug zum Untersuchungsgegenstand;

- Prüfung von explizit dargelegten Datenschutzprofilen;
- Prüfung der Zusammenstellung des Anforderungskatalogs aus den Datenschutzprofilen;
- Prüfung der Vollständigkeit der Umsetzung, um sicherzustellen, dass die Dokumentation zu allen Aspekten des Anforderungskatalogs entsprechende Hinweise zur Umsetzung enthält;
- Stichprobe, ob die dokumentierte Umsetzung korrekt ist. Die Stichprobe muss angemessen sein und besonders sensible Bereiche hinreichend erfassen. Es obliegt dabei dem Auditor, geeignete Schwerpunkte zu setzen und ggf. auf existierende Zertifikate zu verweisen.

### 6.2 Zertifizierung

Insgesamt prüft die Zertifizierungsstelle, ob das Datenschutzaudit gemäß den Vorgaben durchgeführt wurde und vergibt anschließend das Zertifikat.

Die Laufzeiten eines Zertifikats sind identisch zu den Laufzeiten eines ISO 27001-Zertifikats: Drei Jahre Gültigkeit mit jährlichem Überwachungsaudit, bei dem überprüft wird, ob der Prozess „gelebt“ wird und welche Änderungen sich ergeben haben.

### 6.3 Auditoren und Zertifizierungsstellen

Die Zertifizierungsstelle für das Zertifikat für Datenschutz-Management sollten Stellen sein, die in der Lage sind, Managementsysteme zu zertifizieren<sup>15</sup> und eine hinreichende Fachkunde im Bereich des Datenschutzes und der Informationssicherheit vorweisen können. Hierbei bieten sich insbesondere Zertifizierungsstellen für ISO 27001-konforme Informationssicherheits-Managementsysteme an, die gemäß ISO 27006<sup>16</sup> akkreditiert sind.

Die Norm ISO 27006, welche bei ISO 27001-Audits sehr konkrete Anforderun-

<sup>15</sup> beispielsweise nach ISO/IEC 17021: 2006, Konformitätsbewertungsstellen – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren.

<sup>16</sup> ISO/IEC 27006: 2007, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

gen an Prüfumfang und -tiefe stellt, ist dabei sinngemäß zu adaptieren. Die nach ISO 27006 aufgestellten Zertifizierungssysteme der Zertifizierungsstellen, welche eine Grundlage für die Akkreditierung als Zertifizierungsstelle darstellt, sollten eingesetzt werden.

Zudem lizenziert eine Zertifizierungsstelle Auditoren für drei Jahre, die eine hinreichende Erfahrung aus den Bereichen Recht und Technik vorweisen können. Auch hier sollten die Anforderungen aus ISO 27006 entsprechend adaptiert werden.

Aus unserer Sicht sollten die Zertifizierungsstellen privatwirtschaftlich organisiert, bei der Deutschen Akkreditierungsstelle (DAkKS) akkreditiert und hinsichtlich der datenschutzrechtlichen Kompetenz vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) anerkannt sein.

## 7 Ausblick

Der erörterte Ansatz eines Auditierungs- und Zertifizierungsschemas für ein Datenschutz-Management bietet aus unserer Sicht folgende Vorteile:

- Datenschutz wird in einer Institution umfassend und übergreifend etabliert;
- der strukturierte Ansatz gewährleistet eine Vollständigkeit der Maßnahmen – auch unter Einbindung etablierter und akzeptierter Standards der Informationssicherheit;
- durch den in anderen Managementsystemen bewährten Ansatz des Plan-Do-Check-Act-(PDCA-)Zyklus wird eine kontinuierliche Verbesserung ermöglicht;
- Datenschutz auf Prozessebene lässt sich nachhaltig und vergleichbar auditieren und zertifizieren.

Trotz des Fehlens eines Bundesdatenschutzauditgesetzes bestehen die aufgezeigten Möglichkeiten, um vorbildliches Datenschutz-Management zu auditieren und zu zertifizieren.

Gegenwärtig wird das hier vorgestellte Auditierungs- und Zertifizierungsschema für ein Datenschutz-Management in einem Pilot-Audit erprobt.