Christian Prietz, Martin Rost, Julia Stoll

# Prüfverfahren zur datenschutzrechtlichen Zertifizierung

Dieser Artikel stellt die in internationalen Zertifizierungsverfahren gängige Unterscheidung von Prüfkriterien, Prüfsystematik und der Prüfmethoden im Kontext eines datenschutzrechtlichen Zertifizierungsverfahrens dar. Er zeigt anhand datenschutzrechtlicher Zertifizierungsprogramme auf, warum eine Vereinheitlichung der Prüfpraxis in den Datenschutzaufsichtsbehörden anzustreben ist.

## 1 Einleitung

Mit der Anwendung der Datenschutz-Grundverordnung (DS-GVO[1]) sind Zertifizierungen im Datenschutz zu fördern. Datenschutzrechtliche Zertifizierungen umfassen Zusicherungen hinsichtlich der datenschutzkonformen Realisierung von Verarbeitungen personenbezogener Daten. Sie sollen auch als Nachweis[2] dienen, dass zum Zeitpunkt der Zertifizierung, aber auch darüber hinaus, im Gültigkeitszeitraum von maximal drei Jahren (vgl. Art. 42 Abs. 7) diese Zusicherungen eingehalten werden. Die Einhaltung solcher Zusicherungen ist für Verarbeitungstätigkeiten regelmäßig zu prüfen. Des Weiteren müssen die Zusicherungen des Zertifizierungsgegenstands im Einsatz immer in Abhängigkeit von einer konkreten Verarbeitungstätigkeit beurteilt werden. Hieraus resultiert eine Vielzahl an Fragen, wie die Folgenden:

- Welche Prüfkriterien sind relevant und entsprechend heranzuziehen?
- Welche Prüfsystematik ist zu entwickeln?
- Welche Prüfmethoden können angewendet werden?
- Wie lassen sich Ergebnisse solcher Prüfungen datenschutzrechtlich beurteilen?

Die Antworten auf diese vier Fragen machen jede datenschutzrechtliche Prüfung, insbesondere für datenschutzrechtliche Zertifizierungen, aus.

1 Alle nachfolgenden Artikel ohne Nennung der Norm sind solche der DS-GVO.

**Christian Prietz**

ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und Mitglied im Arbeitskreis Zertifizierung sowie im Unterarbeitskreis Prüfkriterien.
E-Mail: cprietz@datenschutzzentrum.de

**Martin Rost**

ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und Leiter der Arbeitsgruppe „Standard-Datenschutzmodell"
E-Mail: martin.rost@datenschutzzentrum.de

**Julia Stoll**

ist Referatsleiterin Informatik, Referat 3.2, beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit. Sie ist Mitglied im Arbeitskreis Zertifizierung, darüber hinaus Leiterin des Unterarbeitskreises Prüfkriterien.
E-Mail: julia.stoll@datenschutz.hessen.de

## 2 Zertifizierungen als spezifische Form der datenschutzrechtlichen Prüfung

Ein Zertifizierungsprogramm umfasst die Beschreibung des Zertifizierungsgegenstands, die dazugehörigen Zusicherungen sowie Prüfkriterien, Prüfsystematik und Prüfmethoden, so dass eine qualifizierte datenschutzrechtliche Beurteilung vorgenommen werden kann. Wenn die Beurteilung des Zertifizierungsgegenstands positiv ausfällt, wird die entsprechende datenschutzrechtliche Zertifizierung erteilt.

Ein Zertifizierungsgegenstand ist eine Verarbeitungstätigkeit oder ein Verarbeitungsvorgang als Teil einer spezifischen Verarbeitung oder eine Komponente einer Verarbeitung innerhalb einer Organisation.[3] Die Grundlage einer Verarbeitungstätigkeit

2 Art. 42 Abs. 1 und 4, Art. 46 Abs. 2 lit. f sowie Art. 83 Abs. 2 lit. j.

3 Hieraus folgt, dass Hersteller sich nur einzelne reale Komponenten im Zusammenhang mit einer konkreten Verarbeitungstätigkeit zertifizieren lassen können. Eine Zertifizierung für eine Komponente im Zusammenhang mit einem abstrakten Einsatzszenario ist hingegen nicht möglich. Weiter folgt, dass ein Hersteller sich nur zertifizieren lassen kann, wenn er für einen bestimmten Verantwortlichen als Auftragsverarbeiter tätig wird.

ist die rechtliche Spezifikation einer Verarbeitung (Art. 4 Nr. 2) personenbezogener Daten (Art. 4 Nr. 1). Die datenschutzrechtlichen Anforderungen, an die Verarbeitung personenbezogener Daten, sind konkret im Zusammenhang mit der betrachteten Verarbeitungstätigkeit und dem Zertifizierungsgegenstand im Einsatz zu sehen.

Eine ordnungsgemäß erteilte Zertifizierung muss den Anspruch haben, dass diese nicht durch eine Datenschutzaufsichtsbehörde beanstandet werden kann; gleiches gilt für den Zertifizierungsgegenstand im konkreten Einsatz. Die Zusicherungen müssen den Zertifizierungsgegenstand abdecken, so dass dieser vollumfänglich geprüft werden kann. Die oben beschriebenen Anforderungen an Prüfverfahren gelten für konkrete und generische Zertifizierungsprogramme, wobei die notwendigen Konkretisierungen bei Letzteren nachgelagert sein müssen.

### 2.1 Abriss der Rahmenbedingungen

Die Unterscheidung von Prüfkriterien, Prüfsystematik und Prüfmethoden ist in internationalen Zertifizierungsverfahren gängig und basiert auf der Anwendung der technischen Normen DIN EN ISO/IEC 17000 und DIN EN ISO/IEC 17011. Diese sind ihrerseits grundlegend, um die technische Norm DIN EN ISO/IEC 17065 anzuwenden.[4] Die Anwendung dieser Norm ist durch ihre Nennung in Art. 43 Abs. 1 lit. b bereits gesetzlich vorgegeben. Gemäß Art. 42 Abs. 5 sind von den zuständigen Datenschutzaufsichtsbehörden Kriterien zu genehmigen. Die Zertifizierungsstellen müssen im Rahmen ihrer Akkreditierung (Art. 43) nachweisen, dass sie befähigt sind, aus der Prüfbarkeit von Kriterien zu einer Beurteilung der Rechtskonformität zu gelangen.[5] Diese Kriterien sind die Prüfkriterien für datenschutzrechtliche Prüfverfahren. Ohne Prüfkriterien hinsichtlich des Anwendungskontexts[6] des Zertifizierungsgegenstands im Einsatz („Zertifizierungsprogramm") kann eine Zertifizierungsstelle nicht akkreditiert werden (Art. 43 Abs. 2 lit. b).

### 2.2 Prüfverfahren für datenschutzrechtliche Zertifizierungen

Ein angemessenes und geeignetes Prüfverfahren muss Prüfergebnisse hinsichtlich der Gültigkeit datenschutzrechtlicher Zusicherungen liefern, anhand derer entschieden werden kann, ob eine Zertifizierung erteilt wird oder ob sie nicht erteilt wird.

Jedes datenschutzrechtliche Prüfverfahren muss sicherstellen, dass der Zertifizierungsgegenstand tatsächlich geprüft und beurteilt werden kann. Dazu sollte ein datenschutzrechtliches Prüfverfahren die folgenden Eigenschaften besitzen:

- Auf der Basis der Prüfkriterien muss die Prüffähigkeit der rechtlichen Anforderungen für den Zertifizierungsgegenstand durch normative SOLL-Vorgaben und IST-Feststellungen gewährleistet werden.
- Die Prüfsystematik muss sowohl die Kontrollierbarkeit von relevanten Komponenten der Verarbeitungstätigkeiten, von Verarbeitungsvorgängen oder einer Verarbeitungstätigkeit im Anwendungskontext gewährleisten, als auch die Prüfbarkeit des Zertifizierungsgegenstands im Einsatz sicherstellen.
- Die Durchführung datenschutzrechtlicher Prüfungen muss die Validierung des Zertifizierungsgegenstands anhand technisch-organisatorischer SOLL-Vorgaben und IST-Feststellungen im Einsatz sicherstellen.
- Prüfergebnisse zum Zertifizierungsgegenstand im Anwendungskontext müssen der datenschutzrechtlichen Beurteilung dienen, so dass festgestellt werden kann, ob die Verarbeitungstätigkeit oder der Verarbeitungsvorgang datenschutzkonform ist.

Ein solches datenschutzrechtliches Prüfverfahren muss jederzeit ausgeführt werden können. Prüfen ist hierbei eine Aktivität, um den Unterschied zwischen SOLL- und IST-Werten festzustellen und somit ein konkretes Prüfergebnis herzustellen. Kontrollieren ist eine dem Prüfen vorausgehende Aktivität, die in Bezug auf den Zertifizierungsgegenstand festlegt, welche Komponenten und Eigenschaften relevant oder nicht relevant sind. Mit dem Bestimmen der relevanten Aspekte wird die Prüfbreite festgelegt.

#### 2.2.1 Datenschutzrechtliche Prüfkriterien

Ein datenschutzrechtliches Prüfkriterium ist ein Merkmal einer datenschutzrechtlichen Anforderung (SOLL-Wert), das für eine konkrete und dokumentierte Verarbeitungstätigkeit (Art. 30) umzusetzen und festzustellen ist (IST-Wert). Somit können drei Ebenen betrachtet werden, an denen vor einer Prüfung die Prüfkriterien auszuweisen sind:

- DS-GVO Anforderungen zur Umsetzung der europäischen Grundrechtecharta (Art. 7 und Art. 8 GRCh),
- generische Maßnahmen zur Umsetzung von DS-GVO Anforderungen, und
- konkrete Maßnahmen zur Umsetzung der generischen Maßnahmen.[7]

Mithin ergeben sich für datenschutzrechtliche Prüfkriterien folgende Eigenschaften:

- Ein Prüfkriterium ist ein Element einer vorausschauenden datenschutzrechtlichen Beurteilung und garantiert die Prüffähigkeit der Verarbeitung in der Zukunft, so dass die Zusicherungen des Zertifizierungsprogramms für die Dauer der Verarbeitung personenbezogener Daten erfüllt werden.
- Ein Prüfkriterium ist grundlegend für die Prüfsystematik. Denn mit der Prüfsystematik sind Erwartungen an Prüfmethoden verknüpft, die ihrerseits die Möglichkeit einer konkreten Prüfung einer Verarbeitungstätigkeit zu eröffnen haben; d.h. ein Prüfkriterium muss die Prüffähigkeit der unmittelbaren Verarbeitung sicherstellen.
- Ein Prüfkriterium muss so gestaltet sein, dass eine in der Vergangenheit liegende Verarbeitung personenbezogener Daten

4 Jedes Zertifizierungsprogramm ist ein Konformitätsbewertungsprogramm mindestens unter Anwendung der genannten technischen Normen. Ein Zertifizierungsgegenstand ist mit einem Programm konform, wenn alle hierin getroffenen Zusicherungen mindestens im Gültigkeitszeitraum der Zertifizierung eingehalten und im Betrieb vorgehalten werden können.

5 Vgl. Akkreditierungsprozess für den Bereich „Datenschutz" gemäß Art. 42, 43 (Version 1.0), siehe hierzu [2]. Im Unterschied zu anderen etablierten Akkreditierungsverfahren, die auf Basis der technischen Norm DIN EN ISO/IEC 17065 durch die Deutsche Akkreditierungsstelle (DAkkS) durchgeführt werden, obliegt es der zuständigen Datenschutzaufsichtsbehörde der akkreditierten Stelle die Befugnis zu erteilen, als Zertifizierungsstelle gemäß Art. 43 tätig zu werden.

6 Anwendungskontexte sind bspw. spezifische Bereiche der Daseinsvorsorge (Elektrizität oder auch Verkehr), Soziales und Gesundheit, innere Sicherheit, Verwaltung sowie Wirtschaft mit Banken und Versicherungen oder auch Bildung und Forschung.

7 Das Standard-Datenschutzmodell („SDM", aktuelle Version: V2b) enthält einen dieser Systematik zugeordneten Katalog mit Maßnahmen zur Umsetzung von Anforderungen der DS-GVO, siehe [3].

datenschutzrechtlich zu beurteilen ist, um auf Dauer eine datenschutzkonforme Verarbeitungen personenbezogener Daten in Systemen und Diensten sicherzustellen.

Im Übrigen müssen Prüfkriterien die Anforderungen des Art. 5 erfüllen.

Als Beispiel fordert die DS-GVO in Art. 5 Abs. 1 lit. a Transparenz. Als generische Maßnahme wird u.a. Protokollierung[8] zur Umsetzung dieser Anforderung genutzt. Die konkrete Umsetzung der Protokollierung umfasst

- den Zeitpunkt, an dem der Protokolleintrag erstellt wurde[9],
- einen Bezeichner für die Entität, die den Protokolleintrag ausgelöst hat, und
- einen Bezeichner für die Aktivität und ihr Ergebnis.

Neben der Protokollierung, die die Prüffähigkeit einer Verarbeitungstätigkeit für die Vergangenheit sicherstellen soll, sind Dokumentation und Spezifikation als weitere generische Maßnahmen zur Gewährleistung und Sicherstellung der Transparenz zu nennen, wie in Art. 5 Abs. 1 lit. a gefordert. Eine Dokumentation sollte für eine Prüfung alle Daten, Komponenten und Prozesse einer Verarbeitungstätigkeit auflisten, beschreiben und die jeweiligen SOLL- und zu erwartenden IST-Werte ausweisen, für die auch die Prüfmethoden anzugeben sind. Des Weiteren ist eine Spezifikation erforderlich, die beispielsweise in Form eines Lasten- und Pflichtenhefts erstellt werden kann. Darin liegen alle normativen und funktionalen Anforderungen des Auftraggebers expliziert vor und der Auftragnehmer macht die entsprechenden Zusicherungen, insbesondere auch in Bezug auf die dauerhafte Sicherstellung der datenschutzrechtlichen Prüffähigkeit in der Zukunft.

### 2.2.2 Datenschutzrechtliche Prüfsystematik

Eine Prüfsystematik für datenschutzrechtliche Zertifizierungen dient der Kontrolle des Zertifizierungsgegenstands, speziell der Zusicherungen im Zertifizierungsprogramm hinsichtlich einer spezifizierten Verarbeitungstätigkeit. Die Prüfsystematik muss daher sicherstellen, dass die Transformation von der Beobachtung, über die Feststellung hin zur datenschutzrechtlichen Beurteilung möglich ist. Dabei ist die Prüftiefe festzulegen, die notwendig ist, um die Wirksamkeit technisch-organisatorischer Maßnahmen sicher bestimmen zu können.

Die datenschutzrechtliche Prüfsystematik muss somit sicherstellen, dass

- der Zertifizierungsgegenstand den datenschutzrechtlichen Anforderungen im Anwendungskontext genügt,
- die verbundene Wahl der Mittel geeignet und angemessen ist, um die Zusicherungen im Zertifizierungsprogramm auf Dauer einzuhalten,
- der Betrieb der inhärenten IT-Systeme und IT-Dienste so kontrolliert ablaufen kann, dass auch unter ggf. notwendigen technischen Anpassungen und Änderungen die Zertifizierungsaussage[10], im Gültigkeitszeitraum der Zertifizierung bestehen bleibt.

Folgendes sollte hinsichtlich der Wahl geeigneter und angemessener Mittel berücksichtigt werden:

a) Auf der Ebene datenschutzrechtlicher Prüfkriterien als rechtliches Erfordernis sind die Grundsätze aus Art. 5, sowie weitere Kriterien der DS-GVO, anzuführen. Es geht um die Frage, welche Mittel werden zur Umsetzung bestimmter und festgelegter datenschutzrechtlicher Anforderungen in Hinblick auf die betrachtete Verarbeitungstätigkeit im Anwendungskontext des Zertifizierungsgegenstands eingesetzt. Bei einer Konzentration auf diese Grundsätze ergibt sich auch ein Kriterium für die Vollständigkeit der normativen Prüfkriterien.
b) Jeder normative Grundsatz muss durch mindestens eine geeignete generische Maßnahme funktional nach dem Stand der Technik umgesetzt werden. Ob eine Maßnahme zur Umsetzung eines Grundsatzes gemäß Art. 5 vorliegt, ist dann eine prüfbare Eigenschaft bzw. ein Prüfkriterium. Daraus ergeben sich beispielsweise folgende Fragen: Welche Maßnahmen, auf einer zunächst generischen Ebene, werden als geeignet und angemessen angesehen? Was bestimmt vorzugsweise die Auswahl der technisch-organisatorischen Maßnahmen?
c) Wenn für diese generischen Maßnahmen jeweils konkrete Eigenschaften technisch spezifiziert sind, lassen sich für konkrete Maßnahmen detaillierte Prüfkriterien aufstellen, welche zu der Frage führen: Wie werden diese technisch-organisatorischen Maßnahmen konkret implementiert?
d) Auf der Ebene der konkreten technisch-organisatorischen Maßnahmen lassen sich darüber hinaus Prüfkriterien mit höher aufgelösten Eigenschaften prüfen.

Für die Punkte a) bis c) wird auf das unter 2.2.1 dargestellte Beispiel der Protokollierung verwiesen. Für d) folgt hieraus, dass es beispielsweise relevant sein kann, in welcher Auflösung die einzelnen Protokolleinträge erfolgen. Für den speziellen Protokolleintrag des Zeitpunktes ergeben sich unter anderem folgende Fragen:

- Was ist die Quelle für die Zeitinformation (Zeitserver)?
- Welche Anforderungen werden an die Zuverlässigkeit der Zeitquelle gestellt?
- Welche Auflösung der Darstellung des Zeitpunktes ist notwendig?

Vergleichbare Fragen sind auch an die anderen Protokolleinträge (Entität, Aktivität und Ergebnis) zu stellen.

Mithin ergeben sich für das Beispiel Transparenz / Protokollierung folgende datenschutzrechtliche Prüfanweisungen vom Allgemeinen zum Besonderen („Top-Down“):

- Erklären Sie, wie Transparenz (Art. 5 Abs. 1 lit. a) hergestellt wird (siehe a)).
- Erklären Sie für den Zertifizierungsgegenstand den Zweck der Protokollierung (siehe b)).
- Zeigen Sie das Zustandekommen des Protokolls und erklären Sie die Protokolleinträge mit Bezug zum Zertifizierungsgegenstand. Lösen Sie dazu eine Aktivität aus, die einen Protokolleintrag erzeugt (siehe c)).
- Zeigen Sie, dass die Auflösung der Zeitnotation mit Bezug zum Einsatz des Zertifizierungsgegenstands angemessen ist (siehe d)).

### 2.2.3 Datenschutzrechtliche Prüfmethoden

Eine datenschutzrechtliche Prüfmethode ist die Art der Nachweiserbringung in der Praxis durch eine oder mehrere Aktivitäten, mittels derer nachgewiesen werden kann, ob eine Zusicherung hinsichtlich der datenschutzrechtlichen Anforderungen

8 Der Begriff der Protokollierung beschreibt hier einzig den Vorgang der Erstellung von Protokolleinträgen, ohne deren Auswertung.

9 An dieser Stelle soll nicht betrachtet werden, ob die Zeit des zu protokollierenden Produktivsystems oder die Zeit des Protokollservers erfasst wird. Dies ist eine Frage der Sicherstellung der Integrität des Protokolleintrags.

10 Synonym zur Siegelaussage einer Datenschutz-Zertifizierung.

beim Einsatz des Zertifizierungsgegenstands im Anwendungskontext technisch sichergestellt und/oder rechtlich gewahrt ist.
Daraus ergibt sich ein grundlegendes Verfahren zur Erstellung datenschutzrechtlicher Prüfmethoden:

1. Die spezifikationsgemäß eingesetzten technisch-organisatorischen Maßnahmen müssen im Einklang mit den datenschutzrechtlichen Anforderungen in der technischen Implementierung sein. Die datenschutzrechtliche Zertifizierung muss die Wirksamkeit der ergriffenen technisch-organisatorischen Maßnahmen nachweisen. Nur dann kann aus technischer Sicht eine datenschutzkonforme Verarbeitung personenbezogener Daten erfolgen.
2. Die eingesetzten IT-Systeme und IT-Dienste müssen den datenschutzrechtlichen Anforderungen im Betrieb auf Dauer genügen.
3. Die IT-Systeme und IT-Dienste müssen aktiv und regelmäßig getestet werden, um auf der technischen Ebene funktionale IST-Werte zu erzeugen, die gegen funktionale SOLL-Werte zu vergleichen sind. Von daher müssen Anwendungs- und Testszenarien frühzeitig auf der Basis der Spezifikation entwickelt werden.
4. Die ermittelten Abweichungen hinsichtlich der Zusicherungen des jeweiligen Zertifizierungsprogramms sind zu bewerten, um die Schwere der Abweichungen festzustellen.
5. Die festgestellten Abweichungen sind unter Berücksichtigung ihrer Schwere datenschutzrechtlich zu beurteilen.
6. Auf der Grundlage der datenschutzrechtlichen Beurteilung sind Entscheidungen zu treffen, welche Anpassungen notwendig sind, um bestehende Zusicherungen des Zertifizierungsprogramms zu wahren.
7. Wenn keine Anpassungen möglich sind, dann ist
   - keine erfolgreiche, oder
   - keine Aufrechterhaltung einer bestehenden Zertifizierung möglich.

Bei einer durchzuführenden Prüfung der konkreten Eigenschaften für die Transparenz am Beispiel der Protokollierung dreht sich die in 2.2.2 dargestellte Vorgehensweise um („Bottom-Up“):

- Zeigen Sie, dass die Auflösung der Zeitnotation mit Bezug zum Einsatz des Zertifizierungsgegenstands im Anwendungskontext angemessen ist (siehe d)).
- Stellen Sie fest, dass das Zustandekommen des Protokolls und der jeweiligen Protokolleinträge mit Bezug zum Zertifizierungsgegenstand korrekt ist (siehe c)).
- Begründen Sie für den Zertifizierungsgegenstand, dass der Zweck der Protokollierung dadurch erfüllt wird (siehe b)).
- Beurteilen Sie, ob die Transparenz (Art. 5 Abs. 1 lit. a) durch den Einsatz der Protokollierung hinreichend hergestellt wird (siehe a)).

## 3 Aktuelle Herausforderung in der Realisierung datenschutzrechtlicher Zertifizierungen

Datenschutzrechtliche Zertifizierungen dürfen nur von akkreditierten Zertifizierungsstellen durchgeführt und betrieben werden. Wie bereits dargestellt, müssen die Kriterien als Teil des Zertifizierungsprogramms durch die zuständige Datenschutzaufsichtsbehörde genehmigt werden. Wie ebenfalls bereits dargestellt, zählen dazu auch die Prüfkriterien, Prüfsystematik und -methoden. Ein Zertifizierungsprogramm kann von der zertifizierenden Stelle selbst entwickelt oder von einem Programmeigner eingekauft werden. Eine Zertifizierungsstelle muss während des Akkreditierungsprozesses nachweisen, dass sie in der Lage ist, vollumfänglich abdeckend datenschutzrechtliche Prüfverfahren umzusetzen und zu betreiben.

Jeder EU-Mitgliedstaat kann entscheiden, wer die Akkreditierung einer Zertifizierungsstelle durchführt. Die DS-GVO sieht vor, dass eine Akkreditierung durch eine nationale Akkreditierungsstelle oder durch die zuständige Datenschutzaufsichtsbehörde durchgeführt wird (Art. 43 Abs. 1). In Deutschland wird die Deutsche Akkreditierungsstelle die Akkreditierung zusammen mit den jeweiligen Datenschutzaufsichtsbehörden der Länder durchführen.[11] Die Deutsche Akkreditierungsstelle ist Mitglied der „European Accreditation" (EA)[12], die u.a. die Normungsprozesse innerhalb der technischen Normen der ISO begleitet. Gleichwohl hat sich die Deutsche Akkreditierungsstelle hinsichtlich einer Europäischen Zusammenarbeit verpflichten müssen, dass sie selbst von der EA auditiert wird.

Zur Realisierung einer datenschutzrechtlichen Zertifizierung sollten sich alle Beteiligten nach den Vorgaben des Europäischen Datenschutzausschusses richten.

Der Europäische Datenschutzausschuss hat in einer Anleitung hinsichtlich der Realisierung datenschutzrechtlicher Zertifizierungen einige Artikel der DS-GVO besonders hervorgehoben.[13] Eine auf dieser Grundlage erstellte rechtliche Spezifikation wird grundsätzlich die Auswahl der technisch-organisatorischen Maßnahmen zur Implementierung einer Verarbeitungstätigkeit beeinflussen. Ob durch diese Hervorhebung die notwendige Spezifikation von datenschutzrechtlichen Prüfverfahren, insbesondere im Zusammenhang mit datenschutzrechtlichen Zertifizierungen, vollumfänglich abdeckt wird, muss nicht sichergestellt sein. Des Weiteren ist es der Europäischen Kommission vorbehalten, mittels delegierter Rechtsakte (Art. 43 Abs. 8) und Durchführungsrechtsakten (Art. 43 Abs. 9), die Ausgestaltung von Zertifizierungen zu beeinflussen.

11 Die rechtliche Grundlage für das Handeln der DAkkS ist die Verordnung (EG) Nr. 765/2008 sowie das Akkreditierungsstellengesetz.

12 https://european-accreditation.org/ (letzter Aufruf: 05.08.2020).

13 Siehe hierzu [4].

## 4 Fazit

Zwischen rechtlicher Spezifikation und dem Einsatz eines Zertifizierungsgegenstands in der IT-Praxis besteht eine in der vorgelegten Darstellung identifizierte „Lücke". Deshalb ist mit der Prüfsystematik ein verbindendes Element zu entwickeln. Die Prüfsystematik transformiert in einem mehrstufigen Prozess datenschutzrechtliche Anforderungen in technische Anforderungen für IT-Systeme und IT-Dienste. Die datenschutzrechtlichen Anforderungen sind durch eine Zertifizierungsstelle oder durch einen Programmeigner in ein geeignetes und angemessenes Zertifizierungsprogramm zu überführen, das Prüfkriterien, -systematik und -methoden beinhaltet. Die konkrete Implementierung der technischen Anforderungen ist schlussendlich die Basis für eine Bewertung und Beurteilung hinsichtlich der datenschutzrechtlichen Konformität.

Die Prüfkriterien als Teil des Zertifizierungsprogramms müssen wegen ihrer Genehmigungspflicht durch die zuständige Datenschutzaufsichtsbehörde (gemäß Art. 42 Abs. 5) den Anforderungen der Behörde genügen. Jede erteilte datenschutzrechtliche Zertifizierung ist somit die Vorwegnahme einer datenschutzrechtlichen Prüfung durch die zuständige Datenschutzaufsichtsbehörde. Aufgrund der föderalen Struktur Deutschlands haben die deutschen Datenschutzaufsichtsbehörden vereinbart, erteilte Zertifizierungen gegenseitig anzuerkennen.[14] Das macht es notwendig, dass die datenschutzrechtlichen Prüfverfahren konvergieren. Unbeachtet dieser notwendigen Konvergenz kann eine datenschutzrechtliche Prüfung durch die Datenschutzaufsichtsbehörde eine Einzelfallentscheidung erforderlich machen, wenn die erteilte Zertifizierung gemäß Art. 83 Abs. 2 lit. j im Rahmen eines Sanktionsverfahrens zu berücksichtigen ist.

## 5 Literatur

[1] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) 2018: Kurzpapier Nr. 9 „Zertifizierung nach Art. 42", verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf (Stand: Dezember 2017, letzter Aufruf: 04.08.2020).

[2] DSK 2019: „Akkreditierungsprozess für den Bereich "Datenschutz" gemäß Art. 42, 43 (Version 1.0), verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf (Stand: März 2019, letzter Aufruf: 04.08.2020.

[3] DSK 2020: Das Standard-Datenschutzmodell – Ein Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, verfügbar unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf (Version 2b, Stand: April 2020, letzter Aufruf: 04.08.2020).

[4] EDPB 2018: Guideline on accreditation of certification bodies under Art. 43 of the General Data Protection Regulation (2016/679) version 3 (04. June 2019), verfügbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf (letzter Aufruf: 04.08.2020).

14 Eine solche Anerkennung erfolgt im Unterschied zur Vorgehensweise auf europäischer Ebene, wo es nach Übereinkunft der Aufsichtsbehörden gerade keine wechselseitige Anerkennung (mutual recognition) geben soll, sofern es sich bei der Zertifizierung nicht um ein Europäisches Datenschutzsiegel nach Art. 42 Abs. 5 handelt.