www.jusletter-it.eu

Georg Borges

Kooperation in der IT-Regulierung durch Zertifizierung

Durch Kooperationen, die Kompetenz und Ressourcen bündeln, können Ergebnisse erzielt werden, die ansonsten nicht oder nicht effizient erzielt würden. Insbesondere für die Regulierung der Informationstechnik hat dies große Bedeutung: Hohe Komplexität führt dazu, dass der Staat seine Aufgaben im Bereich von Normsetzung und Normdurchsetzung nicht effizient wahrnehmen kann. Dieser Befund ist in der Praxis durch vielfältige Regulierungsdefizite belegt. Ein aktuelles Beispiel liefert der Datenschutz, in dem hohe Rechtsunsicherheit beklagt wird und Rechtsdurchsetzungsdefizite offen eingestanden sind. Es liegt nahe, dass eine effektive und zugleich effiziente Regulierung nur durch Kooperation zwischen Staat (Gesetzgeber, Aufsicht) und Bürger, insbesondere der Privatwirtschaft, erreicht werden kann. Eine Möglichkeit der Regulierung durch Kooperation kann ein System der Zertifizierung darstellen. Zertifizierungen in den unterschiedlichsten Ausprägungen sind weit verbreitet, gerade im technischen Bereich, namentlich der Informationstechnologie. Ihre rechtliche Bedeutung ist jedoch weitgehend unklar. Das Papier beschreibt die Voraussetzungen und Leistungen einer rechtlichen Regulierung durch sog. Compliance-Zertifizierung. Gemeint ist eine Zertifizierung, die auf die Erfüllung gesetzlicher Anforderungen gerichtet ist und deshalb als Kooperation im Bereich der rechtlichen Regulierung anzusehen ist. Die Untersuchung erfolgt am Beispiel der datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung.

Collection: Conference Proceedings IRIS 2015; Peer Reviewed – Jury
LexisNexis Best Paper Award of IRIS2015
Category: Articles
Field of law: Data Protection
Region: Germany

Citation: Georg Borges, Kooperation in der IT-Regulierung durch Zertifizierung, in: Jusletter IT 26. Februar 2015 – IRIS

Inhaltsübersicht

1 Einführung

[Rz 1] Der Grundgedanke der Kooperation besteht darin, durch Bündelung von Kompetenz und Ressourcen ein Ergebnis zu erreichen, das die Kooperationspartner alleine nicht oder nicht effizient erzielen könnten. Diese Zielsetzung hat für die Regulierung von Informationstechnik große Bedeutung. Wegen der hohen Komplexität informationstechnischer Systeme steht deren Regulierung, d.h. die Schaffung verbindlicher Anforderungen und die Kontrolle deren Einhaltung, sowohl im Bereich der Normsetzung (Gesetzgebung, Standardisierung) als auch im Bereich der Normdurchsetzung (behördliche Aufsicht, Haftung bei Verstößen, Durchsetzungsrechte von Beteiligten) vor so hohen Herausforderungen, dass der Staat diese Aufgaben alleine nicht effizient bewältigen kann. Eine Möglichkeit der Regulierung durch Kooperation kann ein System der Zertifizierung darstellen. Zertifizierungen in den unterschiedlichsten Ausprägungen sind weit verbreitet, nicht zuletzt in der Informationstechnologie.

[Rz 2] Von besonderem Interesse ist in diesem Zusammenhang die sog. Compliance-Zertifizierung. Gemeint ist eine Zertifizierung, die die Erfüllung gesetzlicher Anforderungen bestätigt. Soweit eine solche Zertifizierung rechtliche Folgen auslösen soll, kann sie eine Kooperation im Bereich der rechtlichen Regulierung darstellen. Die Compliance-Zertifizierung wird derzeit im Bereich des Datenschutzes, speziell bei der Auftragsdatenverarbeitung, intensiv diskutiert. Bei der Auftragsdatenverarbeitung ist die Sicherheit der Datenverarbeitung von großer Bedeutung, die durch staatliche Aufsicht, vor allem aber durch Überwachungsmaßnahmen der Beteiligten gesichert werden soll. Da diese Überwachung bei modernen Formen der Datenverarbeitung, namentlich beim Cloud Computing, Schwierigkeiten aufwirft, soll die Zertifizierung eine effiziente Überwachung der Sicherheit ermöglichen.

[Rz 3] Nachfolgend werden am Beispiel der Auftragsdatenverarbeitung wesentliche Grundfragen der Regulierung durch Zertifizierung als Zusammenwirken staatlicher und privater Tätigkeit erörtert.

2 Zertifizierung und Auftragsdatenverarbeitung

2.1 Die Auftragsdatenverarbeitung

[Rz 4] Die Nutzung von IT-Diensten externer Anbieter erfolgt datenschutzrechtlich regelmäßig auf der Grundlage einer Auftragsdatenverarbeitung. Dies gilt sowohl für traditionelles IT-

Outsourcing wie für moderne IT-Dienstleistungen, namentlich Cloud Computing.

[Rz 5] Bei der Auftragsdatenverarbeitung ist die durch den Dienstleister erfolgende Datenverarbeitung gemäß § 3 Abs. 8 S. 3 BDSG zulässig, wenn die in § 11 BDSG geregelten Voraussetzungen der Auftragsdatenverarbeitung erfüllt sind. Danach muss die Auftragsdatenverarbeitung auf einem schriftlichen Vertrag zwischen Auftraggeber und Auftragnehmer beruhen, der die in § 11 Abs. 2 S. 2 Nr. 1 BDSG geregelten Elemente enthält und ein Weisungsrecht des Auftraggebers vorsieht. Außerdem muss der Auftraggeber den Dienstleister gemäß § 11 Abs. 2 S. 1 BDSG sorgfältig auswählen und sich gemäß § 11 Abs. 2 S. 4 BDSG von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Diese in § 9 BDSG geregelten Maßnahmen betreffen die Sicherheit der Datenverarbeitung einschließlich des Schutzes gegen unbefugten Zugriff.

2.2 Die Kontrollpflicht und moderne IT-Dienste

[Rz 6] Die Pflicht des Auftraggebers nach § 11 Abs. 2 S. 4 BDSG wird zutreffend als eine Pflicht zur Kontrolle des Auftragnehmers angesehen,[1] die auch eine Kontrolle der technischen Maßnahmen vor Ort, d.h. eine Inspektion des Rechenzentrums und der Rechner, auf denen die Datenverarbeitung stattfindet, einschließt.[2] Die Notwendigkeit einer Kontrolle vor Ort ist im Grundsatz richtig,[3] da sich die Überprüfung ansonsten auf die Entgegennahme von Angaben des IT-Dienstleisters beschränkte.[4] Dadurch würde aber ein Anreiz für IT-Dienstleister geschaffen, die Durchführung der unter Umständen sehr aufwendigen technischen Maßnahmen lediglich zu behaupten, sie aber in der Praxis nicht durchzuführen. Die Sicherheit der personenbezogenen Daten vor Missbräuchen wäre dann nicht gewährleistet.

[Rz 7] Diese Pflicht, nicht zuletzt die Erforderlichkeit einer Kontrolle vor Ort, ist jedoch für viele potenzielle Nutzer von IT-Dienstleistungen, insbesondere von Cloud Computing, nicht in zumutbarer Weise zu erfüllen.[5] Bei kleinen Unternehmen fehlt es meist bereits an der erforderlichen Sachkunde, so dass für diese Kontrolle ein Dienstleister eingeschaltet werden müsste.[6] Vor allem aber ist die Kontrollpflicht, wenn sie durch jeden Nutzer von IT-Dienstleistungen durchgeführt wird, häufig ineffizient.[7] Dies gilt insbesondere beim Cloud Computing: Dieselbe Datenverar-

---

1 Borges/Brennscheidt in: Borges/Schwenk (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, Heidelberg (2012), S. 43 ff. (65); Brennscheidt, Cloud Computing und Datenschutz, Baden-Baden (2013), S. 98; Heckmann, jurisPK-Internetrecht, Saarbrücken, 3. Auflage (2011), Kap. 9 RN 656.1; Weichert, DuD 2010, 679 (683).

2 Kompetenzzentrum Trusted Cloud, Arbeitsgruppe «Rechtsrahmen des Cloud Computing» — Thesenpapier «Datenschutzrechtliche Lösungen für Cloud Computing» (Oktober 2012), http://trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf, S. 7 f.; Borges/Brennscheidt (FN 1), S. 43 (65); Heidrich/Wegener, MMR 2010, 803 (806); Schuster/Reichl, CR 2010, 38 (42); Wedde, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 4. Auflage (2014), § 11 RN 29.

3 Borges, in BSI (Hrsg.), Informationssicherheit stärken — Vertrauen in die Zukunft schaffen, Gau-Algesheim (2013), S. 11 (19 f.).

4 Borges, DuD 2014, 164 (166). Für ausreichend erachten dies allerdings wohl Gola/Schomerus, BDSG Bundesdatenschutzgesetz — Kommentar, München, 11. Auflage (2012), § 11 Rn. 21 (Fragebögen als ausreichende Kontrollmaßnahme).

5 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), S. 8; BITKOM-Leitfaden Cloud Computing — Evolution in der Technik, Revolution im Business, http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf, S. 52; Borges, DuD 2014, 164 (166); Gola/Schomerus (FN 4), § 11 RN 21.

6 Borges, DuD 2014, 164 (166); Brennscheidt (FN 1), S. 103; Schuster/Reichl, CR 2010, 38 (42).

7 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), S. 8. Borges, DuD 2014, 164 (166).

beitungsanlage des Cloud-Anbieters müsste durch eine Vielzahl von Cloud-Nutzern kontrolliert werden, jeder Cloud-Nutzer müsste eine Vielzahl von Datenverarbeitungsanlagen überwachen.[8]

2.3 Das Konzept der Compliance-Zertifizierung für Auftragsdatenverarbeitung

[Rz 8] Als geeignete Lösung für das Problem der Überwachung bei der Auftragsdatenverarbeitung, insbesondere beim Cloud Computing, wird verbreitet die Erfüllung der Kontrollpflicht durch eine Zertifizierung angesehen.[9] Danach erfolgt die in § 11 Abs. 2 S. 4 BDSG gebotene Kontrolle durch einen unabhängigen Dritten, der für die Cloud-Nutzer die Überprüfung vornimmt und die Einhaltung der rechtlich gebotenen Maßnahmen durch ein Zertifikat oder Testat bezeugt.[10]

[Rz 9] In der aktuellen Diskussion kommt dem Thesenpapier «Datenschutzrechtliche Lösungen für Cloud Computing» der Arbeitsgruppe «Rechtsrahmen des Cloud Computing» [11] besondere Bedeutung zu. Die Arbeitsgruppe, die mit Vertretern aus Wissenschaft, Praxis und insbesondere Datenschutzaufsichtsbehörden besetzt ist,[12] beschreibt in diesem Papier in insgesamt 10 Thesen das Konzept einer datenschutzrechtlichen Zertifizierung einschließlich der rechtlichen Bedeutung des Zertifikats (Testat) und der wesentlichen Merkmale des Zertifizierungsverfahrens.

[Rz 10] Das Konzept sieht im Kern vor, dass der Auftraggeber die Pflicht zur Überprüfung des Auftragnehmers dadurch erfüllen kann, dass er ein Testat prüft, das die Gewährleistung der datenschutzrechtlichen Anforderungen durch den Cloud-Anbieter bestätigt.[13] Das Thesenpapier verwendet den Begriff des Testats,[14] offensichtlich um eine begriffliche Nähe zur Bestätigung rechtlicher Anforderungen, etwa dem Testat nach § 322 HGB, zu suchen und um sich von Gütesiegeln abzugrenzen.

[Rz 11] Das Konzept enthält wesentliche Grundlagen der Zertifizierung. So sieht es vor, dass die Zertifizierung nur durch eine unabhängige Stelle erfolgen kann,[15] die eine hinreichende fachliche und persönliche Eignung aufweist.[16] Die Eignung der zertifizierenden Stelle soll durch eine Akkreditierung nachgewiesen werden müssen.[17] Die ordnungsgemäße Durchführung der Zer-

---

8 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), S. 8; Borges, DuD 2014, 164 (166); Selzer, DuD 2013, 215 (216).

9 Arbeitskreise Technik und Medien, Orientierungshilfe — Cloud Computing (September 2011), http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, S. 9; Borges/Brennscheidt (FN 1), S. 67 f.; Brennscheidt (FN 1), S. 105 f.; Eckhardt in: Köhler-Schute (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen, Berlin (2011), S. 166 ff. (187); Heckmann, in: Hill/Schliesky (Hrsg.), Innovationen im und durch Recht, Baden-Baden (2010), S. 107; Hennrich, CR 2011, 546 (552); Rechtliche Anforderungen an Cloud Computing — Sichere Cloud-Dienste (November 2011), http://www.eurocloud.de/wp-content/blogs.dir/5/files/anford_recht_beicloudcomputing_v1.pdf, S. 40; Marnau/Schirmer/Schlehan/Schunter, DuD 2011, 333 (336); Reindl, in: Taeger/Wiebe (Hrsg.), Inside the Cloud, Edewecht (2009), S. 449; Schröder/Haag, ZD 2011, 147 (149); Selzer, DuD 2013, 215 (218 f.); Weichert, DuD 2010, 679 (683).

10 Borges in: BSI (Hrsg.) (FN 3), S. 11 (19 f.); Borges/Brennscheidt (FN 1), S. 67 f.; Brennscheidt (FN 1), S. 105 f.

11 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2). Siehe dazu Borges, DuD 2014, 165 (166 ff.).

12 Siehe auch AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), S. 22.

13 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 5, S. 11.

14 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), S. 12 f.

15 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 5, S. 12.

16 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 8, S. 17.

17 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 8, S. 18.

tifizierung soll darüber hinaus durch eine zivilrechtliche Haftung der Zertifizierungsstelle für fehlerhafte Prüfungen und Zertifizierungen gesichert werden.[18] Das Konzept zielt auf eine gesetzliche Regelung der Zertifizierung ab, die in der europäischen Datenschutzgrundverordnung erfolgen soll.[19]

3 Datenschutz-Zertifizierungen in der Praxis

[Rz 12] Zertifizierungen mit Bezug zum Datenschutz sind in der Praxis auch auf der Grundlage geltenden Rechts weit verbreitet. Die Stiftung Datenschutz der Bundesrepublik Deutschland veröffentlicht auf ihrer Website eine Sammlung von 32 Zertifizierungen,[20] die sich auf Datenschutz beziehen. Aus dieser beeindruckenden Zusammenstellung wird vor allem die Heterogenität des Angebots an Datenschutz-Zertifizierungen deutlich.

[Rz 13] Das Anwendungsfeld der Datenschutz-Zertifizierung geht jedoch noch weit darüber hinaus. In der Praxis bieten zahlreiche Dienstleister Zertifizierungen an, deren Standards vom Prüfer selbst entwickelt oder mit dem Kunden, der die Zertifizierung beauftragt, vereinbart werden. Bei den gegenwärtig angebotenen Zertifizierungen ist oft unklar, welche Standards der Prüfung zugrunde gelegt werden und welchen Umfang die Prüfung hat.

[Rz 14] Allerdings gibt es einige Initiativen, die auf eine Prüfung anhand eines festgelegten Prüfungsstandards abzielen, der die Erfüllung der gesetzlichen Anforderungen umfasst. Der Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD) hat gemeinsam mit der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) den Datenschutzstandard «DS-BvD-GDD-01»[21] und ein darauf basierendes Datenschutzsiegel speziell für die Auftragsdatenverarbeitung entwickelt.[22] Der Standard nimmt für sich in Anspruch, die durch den Auftragnehmer zu erfüllenden Anforderungen des BDSG vollständig zu beschreiben.[23]

[Rz 15] Die vom EuroCloud Deutschland eco e.V. entwickelte «EuroCloud Star Audit»-Zertifizierung[24] führt, basierend auf einem Punktesystem, zu einer Bewertung von bis zu fünf Sternen.[25] EuroCloud nimmt für sich in Anspruch, dass bereits bei einer 1-Stern-Zertifizierung die untersuchten vertraglichen Vereinbarungen den Anforderungen des BDSG genügen.[26] Allerdings wird nicht deutlich, ob mit der Vergabe des Gütesiegels auch zertifiziert wird, dass der Dienst den Anforderungen des § 9 BDSG entspricht.[27]

[Rz 16] Das ULD (Unabhängiges Landeszentrum für Datenschutz des Landes Schleswig-Holstein)

---

18 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 8, S. 18.

19 AG «Rechtsrahmen des Cloud Computing», Thesenpapier (FN 2), These 10, S. 21.

20 Stiftung Datenschutz, Übersicht zu Zertifizierungen und Gütesiegeln im Datenschutz — 5. Dezember 2014, https://stiftungdatenschutz.org/wp-content/uploads/2014/12/SDS-Zertifizierungsu%CC%88bersicht-20-11-14.pdf.

21 Standard «Anforderungen an Auftragnehmer nach § 11 BDSG» — Datenschutzstandard DS-BvD-GDD-01, http://www.dsz-audit.de/wp-content/uploads/GDD-BvD-DATENSCHUTZSTANDARD-DS-BVD-GDD-01-V1-0.pdf.

22 Lepperhoff/Jaspers, MMR 2013, 617; Staub, DuD 2014, 159 (161).

23 Lepperhoff/Jaspers, MMR 2013, 617; Staub, DuD 2014, 159 (161).

24 Giebichenstein/Weiss, DuD 2011, 338.

25 Giebichenstein/Weiss, DuD 2011, 338 (339); Weiss, DuD 2014, 170 (173).

26 Giebichenstein/Weiss, DuD 2011, 338 (340).

27 Brennscheidt (FN 1), S. 112.

bietet ein Datenschutz-Gütesiegel für Produkte an.[28] Maßgeblich für den Kriterienkatalog des ULD Gütesiegels sind das BDSG sowie das Landesdatenschutzgesetz Schleswig-Holstein, das TKG und das TMG.[29] Das Gütesiegel des ULD war Vorbild für das europäische Gütesiegel «European Privacy Seal» (EuroPriSe), dessen Kriterienkatalog auf der Datenschutzrichtlinie basiert.[30]

[Rz 17] In der Praxis haben Zertifizierungen nach ISO-Standards, insbesondere nach der Standardfamilie ISO/IEC 2700x große Bedeutung. Es ist jedoch nicht gesichert, dass eine Zertifizierung etwa nach ISO/IEC 27001 die datenschutzrechtlichen Anforderungen umfassend erfüllt. Umso mehr ist der neue Standard ISO/IEC 27018 von Interesse, der speziell für Cloud-Dienste entwickelt wurde und für sich in Anspruch nimmt, die Anforderungen der europäischen Datenschutz-Richtlinie umzusetzen.[31] Allerdings ist derzeit noch unklar, ob der Standard eine vollständige Berücksichtigung der datenschutzrechtlichen Anforderungen nach dem BDSG gewährleistet.

[Rz 18] Im Pilotprojekt «Datenschutz-Zertifizierung von Cloud-Diensten», das seit November 2013 vom Kompetenzzentrum Trusted Cloud im Auftrag des BMWi durchgeführt wird, sollen auf der Grundlage des Konzepts der AG «Rechtsrahmen des Cloud Computing» die Einzelheiten einer Datenschutz-Zertifizierung von Cloud-Diensten erarbeitet werden. Im Rahmen des Projekts wird ein Prüfstandard für Cloud-Dienste auf der Grundlage von ISO/IEC 27018 entwickelt, der Anforderungen des BDSG umsetzen soll.[32]

4 Compliance-Zertifizierung und Abgrenzungen

[Rz 19] Der Überblick zeigt, dass derzeit eine Vielzahl von Datenschutz-Zertifizierungen angeboten wird, deren Gegenstand, Voraussetzung und rechtliche Bedeutung jedoch oft unklar sind. Es bietet sich daher an, zwischen Compliance-Zertifizierungen und Gütesiegeln zu unterscheiden.

[Rz 20] Mit dem Begriff der Compliance-Zertifizierung ist die Zertifizierung der Erfüllung gesetzlicher Anforderungen gemeint. Als Gegenbegriff soll hier der Begriff der (schlichten) Zertifizierung oder des Gütesiegels verwendet werden. Auch der Begriff des Gütesiegels ist nicht verbindlich definiert. Gemeint sind Zertifizierungen über die Einhaltung von Qualitätsmerkmalen, die aber nicht notwendig einer gesetzlichen Grundlage bedürfen und in aller Regel auch nicht hierauf beruhen.

[Rz 21] Die hier getroffene Unterscheidung folgt allein dem Gegenstand und der Aussage des Zertifikats, da sich hieraus auch die unterschiedliche rechtliche Bedeutung ergibt. Compliance-Zertifikate sind aufgrund ihres spezifischen Gegenstands ein Spezialfall des Zertifikats. Die gesetzliche Grundlage und das Verfahren, das zur Erteilung des Zertifikats führt, sind hiervon zunächst unabhängig.

---

28 Weichert, in Neudörffer (Hrsg.), ITK-Kompendium 2010, Frankfurt a.M. (2009), S. 274 (276).

29 Weichert, in Neudörffer (Hrsg.) (FN 28), S. 274 (278).

30 Weichert, in Neudörffer (Hrsg.) (FN 28), S. 274 (276).

31 ISO/IEC 27018: Information technology — Security techniques — Code of practice for personally identifiable information (PII) in public clouds acting as PII processors.

32 Siehe zum Pilotprojekt auch die weiterführenden Informationen auf http://trusted-cloud.de/2008.php.

5 Notwendigkeit einer gesetzlichen Regelung der Compliance-Zertifizierung

[Rz 22] Gütesiegel wie Compliance-Zertifikate können hinsichtlich Voraussetzungen und Rechtsfolgen intensiv rechtlich geregelt sein, können aber auch ohne gesetzliche Grundlage vergeben werden. Entsprechend kann es nicht verwundern, wenn bei den Datenschutz-Aufsichtsbehörden derzeit eine erhebliche Skepsis gegenüber den herkömmlichen Zertifizierungen herrscht. So weist die von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten herausgegebene Orientierungshilfe Cloud Computing darauf hin, dass eine Zertifizierung nach ISO/IEC 27001 einen «wichtige[n] Baustein für einen Prüfnachweis» darstelle, eine umfassende datenschutzrechtliche Prüfung aber nicht zertifiziert werde. Daher seien weitere Nachweise erforderlich.[33]

[Rz 23] Compliance-Zertifizierungen benötigen jedoch aus Gründen der Rechtssicherheit regelmäßig eine gesetzliche Regelung. Dies wird am Beispiel der Auftragsdatenverarbeitung besonders sichtbar. Die durch die Zertifizierung angestrebte Wirkung ist nach dem Konzept der AG «Rechtsrahmen des Cloud Computing» nicht etwa eine Bindung der Aufsichtsbehörden. Vielmehr soll, wie dargestellt, der Auftraggeber sich auf die Zertifizierung verlassen können und im Hinblick auf die im Rahmen der Zertifizierung erfolgte Überprüfung der technischen und organisatorischen Maßnahmen auf eine eigene Überprüfung der technischen und organisatorischen Maßnahmen des Auftragnehmers verzichten können.

[Rz 24] Dies ist auch ohne ausdrückliche gesetzliche Regelung möglich. So kann die Überprüfungspflicht nach § 11 Abs. 2 Nr. 4 BDSG nach herrschender Ansicht der Literatur bereits nach den geltenden Normen des BDSG durch das Vertrauen auf das Testat eines geeigneten Zertifizierers erfüllt werden.[34] Da diese Möglichkeit aber im BDSG nicht ausdrücklich angeordnet ist, besteht insoweit Rechtsunsicherheit.[35] Daher sieht das Konzept der AG «Rechtsrahmen des Cloud Computing» vor, dass diese Wirkung des Zertifikats im Gesetz ausdrücklich festgelegt wird.[36]

[Rz 25] Die gesetzliche Festlegung einer solchen Rechtsfolge ist aber nur sinnvoll, wenn auch hinsichtlich der Voraussetzungen für die Erteilung eines solchen Zertifikats Klarheit besteht. Entsprechend fordert die AG «Rechtsrahmen des Cloud Computing» eine umfassende rechtliche Regelung auch der Voraussetzungen der Zertifizierung.[37]

6 Die Compliance-Zertifizierung in der Datenschutz-Grundverordnung

[Rz 26] Die Datenschutz-Grundverordnung (DSGVO) wird voraussichtlich eine gesetzliche Regelung zur Zertifizierung enthalten. Zwar enthält der Entwurf der EU-Kommission zur DSGVO[38]

---

33 *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe Cloud Computing, Version 2.0, Stand 9. Oktober 2014, Ziff. 3, S. 11.

34 AG «Rechtsrahmen des Cloud Computing» — Thesenpapier (FN 2), S. 12; Borges (FN 8), S. 19 f.; Brennscheidt (FN 1), S. 112; Gola/Schomerus (FN 4), § 11 RN 21; Weichert, DuD 2010, 679 (683).

35 Borges (FN 5), S. 20.

36 AG «Rechtsrahmen des Cloud Computing» — Thesenpapier (FN 2), S. 13.

37 AG «Rechtsrahmen des Cloud Computing» — Thesenpapier (FN 2), S. 13.

38 Siehe Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 25. Januar 2012, KOM (2012) 11 endg., 2012/0011 (COD), Änderungsanträge 237 f., S. 155 f. sowie Änderungsantrag 51, S. 46, zu Erwägungsgrund 77.

keine Aussage darüber, ob die Überprüfung durch eine Zertifizierung ersetzt werden kann.Allerdings enthält der Entwurf in Art. 39 eine — sehr allgemeine — Bezugnahme auf Zertifizierungen.

[Rz 27] Im Gesetzgebungsverfahren zur DSGVO sind wesentlich weitergehende Vorschläge zur datenschutzrechtlichen Zertifizierung erarbeitet worden. So sieht der am 12. März 2014 verabschiedete Entwurf des Europäischen Parlaments zur DSGVO eine umfangreiche Regelung zur Zertifizierung in Art. 39 DSGVO vor.[39] Auch der Ministerrat befürwortet eine intensivere Regelung der Zertifizierung in der DSGVO. Im aktuellen Entwurf der italienischen Ratspräsidentschaft vom 3. Oktober 2014[40] wird die Ergänzung des Art. 39 durch einen Art. 39a vorgeschlagen, in dem die Anforderungen an die Zertifizierung und das zugrundeliegende Zertifizierungsverfahren näher geregelt werden.

[Rz 28] Inwieweit die DSGVO, sofern sie erlassen wird, in der endgültigen Fassung eine Regelung zur Zertifizierung enthalten wird, die das Problem des Kontrollerfordernisses anspricht, ist derzeit nicht abzusehen.

7 Zertifizierung als private Wirtschaftstätigkeit

[Rz 29] Ein Kernelement der Compliance-Zertifizierung als Kooperation in der Regulierung betrifft die Frage, ob die Zertifizierung staatlichen Stellen vorbehalten ist oder durch private Stellen erfolgen soll. In Bezug auf die Datenschutz-Grundverordnung divergieren die bisherigen Entwürfe des Parlaments und des Ministerrats. Der Vorschlag des EU-Parlaments für einen neuen Art. 39 Abs. 1d DSGVO sieht vor, dass die Zertifizierung durch die Aufsichtsbehörde erteilt wird,[41] das Parlament scheint sich also für eine ausschließlich hoheitliche Zertifizierung auszusprechen.

[Rz 30] Eine deutlich andere Regelung sieht der aktuelle Entwurf der italienischen Ratspräsidentschaft[42] zu einem Art. 39a DSGVO vor: Nach Art. 39a Abs. 1 muss die Zertifizierungsstelle unabhängig sein und über eine hinreichende Sachkunde verfügen. Sie muss weiterhin auch akkreditiert sein. Die Voraussetzungen der Akkreditierung sind in Art. 39a Abs. 2 DSGVO genannt. Der Entwurf des Ministerrats geht also davon aus, dass die Zertifizierung jedenfalls auch eine Aufgabe privater, akkreditierter Zertifizierungsstellen ist.

[Rz 31] Die AG «Rechtsrahmen des Cloud Computing» und das Pilotprojekt «Datenschutz-Zertifizierung» sprechen sich in ihrem gemeinsamen Papier mit Nachdruck dafür aus, dass eine Zertifizierung jedenfalls auch durch private Stellen erfolgen kann[43].

[Rz 32] Die im Papier genannten Gründe überzeugen. Technische Prüfungen und Zertifizierungen erfolgen seit jeher in hohem Maße durch private Stellen. Staatliche Stellen allein können die erforderlichen Kapazitäten nicht aufbauen. Vor allem aber kann sich durch die Einbeziehung

---

39 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD) (Ordentliches Gesetzgebungsverfahren: erste Lesung).

40 Ratsdokument Nr. 13772/14 vom 3. Oktober 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT.

41 Vgl. oben FN 39.

42 Ratsdokument Nr. 13772/14 vom 3. Oktober 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT.

43 AG «Rechtsrahmen des Cloud Computing» / Pilotprojekt «Datenschutz-Zertifizierung für Cloud-Dienste»: «Datenschutz-Zertifizierung durch private Stellen.»; abrufbar unter http://www.trusted-cloud.de/.

privater Zertifizierer ein Markt für Zertifizierungen entwickeln, der in einem Angebot kostengünstiger Zertifizierung mündet. Es ist daher sehr zu hoffen, dass sich im weiteren Verlauf des europäischen Gesetzgebungsverfahrens die Position des Ministerrats durchsetzen wird.

8 Fazit

[Rz 33] Compliance-Zertifizierungen werden im Bereich des Datenschutzes zu Recht als ein wichtiges Instrument einer kooperativen Regulierung von Informationstechnologie entwickelt. Durch die Einbeziehung privatwirtschaftlicher Elemente wie die Nutzung von Standards, die etwa durch die Wirtschaft oder Standardisierungsorganisationen entwickelt werden, und ebenso durch die Einbeziehung von Unternehmen als Zertifizierungsstellen können die Kompetenz der Privatwirtschaft eingebunden und Marktmechanismen zur Erzielung effizienter Regulierungsmechanismen genutzt werden. Die staatliche Mitwirkung in Form einer Gesetzgebung, die die Rahmenbedingungen für die Zertifizierung festlegt, ist ein wichtiges Mittel, um die für den praktischen Erfolg der Compliance-Zertifizierung unabdingbare Rechtssicherheit zu schaffen.

Georg Borges, Universiätsprofessor, Universität des Saarlandes, Institut für Rechtsinformatik, Lehrstuhl für Bürgerliches Recht, Rechtstheorie und Rechtsinformatik, Campus A5 4, 66123 Saarbrücken, DE, georg.borges@uni-saarland.de; http://it-recht.uni-saarland.de