DIE DATENSCHUTZ-GRUNDVERORDNUNG. POTENTIALE FÜR PRAXISGERECHTEN DATENSCHUTZ

Georg Borges

Universitätsprofessor, Universität des Saarlandes, Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie; geschäftsführender Direktor, Institut für Rechtsinformatik
Campus A5 4, 66123 Saarbrücken, Deutschland, DE
ls-borges@uni-saarland.de; http://www.rechtsinformatik.saarland

Schlagworte: ***DSGVO, Cloud Computing, Trusted Cloud-Datenschutzprofil für Cloud-Dienste, Compliance-Zertifizierung***

Abstract: *Die DSGVO stellt einen Meilenstein in der Entwicklung des Datenschutzrechts dar, da sie unmittelbar anwendbares einheitliches Datenschutzrecht für die gesamte Union bringt. Inhaltlich steht sie in der Tradition der Europäischen Datenschutz-Richtlinie von 1995 und verzichtet auf grundlegende Änderungen des Datenschutzrechts. Zu den innovativen Elementen der DSGVO gehört die Regelung zur Zertifizierung, die ohne Vorbild ist. Die Datenschutz-Zertifizierung ist für moderne Formen der Datenverarbeitung wie Cloud Computing von besonderer Bedeutung. Der Beitrag zeigt das Potential der Zertifizierung auf und analysiert die Regelung der DSGVO.*

1. Erwartungen an die DSGVO

Die im April 2016 erlassene Datenschutz-Grundverordnung (DSGVO) wird ab Mai 2018 unmittelbar anwendbar sein. Damit gilt in der gesamten Union erstmals ein einheitliches Datenschutzrecht. Der Erlass der DSGVO wurde ganz überwiegend begrüßt, gar gefeiert, entsprechend wurden hohe Erwartungen formuliert. Ob die DSGVO wirklich ein Jahrhundertwerk ist, wird sich spätestens ab 2018 im Realitätstest zeigen. Aber ganz sicher ist die DSGVO ein Meilenstein in der Entwicklung des Datenschutzrechts. Dies gilt nicht nur für Europa, sondern weltweit, da schon jetzt absehbar ist, dass die DSGVO die datenschutzrechtliche Dikussion in vielen Ländern weltweit beeinflusst.

Die Frage, ob die DSGVO den Erwartungen gerecht werden kann, kann hier nur exemplarisch untersucht werden. Mit der Notwendigkeit der Auswahl geht eine starke Macht einher, die Auswahl gibt das Ergebnis weitgehend vor. Daher soll hier nicht der Versuch einer Bewertung der DSGVO als solcher unternommen werden. Vielmehr wird, dies sei vorausgeschickt, mit der Datenschutz-Zertifizierung ein Bereich vorgestellt, in dem die DSGVO einen erheblichen Fortschritt im Datenschutzrecht bewirken kann.

2. Die Bedeutung der Datenschutz-Zertifizierung für Cloud Computing

2.1. Cloud Computing und Auftragsverarbeitung

Die Datenschutz-Zertifizierung hat besondere Bedeutung für Cloud Computing und damit für die moderne Datenverarbeitung insgesamt, da sich Cloud Computing zu einer wesentlichen technischen und organisatorischen Grundlage der Datenverarbeitung entwickelt. Der Erfolg des Cloud Computing ist nicht überraschend: Durch die gemeinsame Nutzung von Ressourcen können erhebliche Synergien geschaffen werden. In vielen Bereichen – insbesondere für Kleinunternehmen oder Verbraucher – wird überhaupt erst die Nutzung von Hochtechnologie der Datenverarbeitung ermöglicht.

Diese Vorteile können jedoch nur dann in vollem Maße zur Geltung gebracht werden, wenn Datenschutz auch im Cloud Computing gewährleistet ist. Datenschutz bedeutet im Zusammenhang mit Cloud-Diensten, dass die

Daten beim Cloud-Anbieter nicht weisungswidrig verarbeitet oder weitergegeben werden und nicht zuletzt, dass Unbefugte keinen Zugriff hierauf erhalten.

Dieses Erfordernis hat beim Cloud Computing, das typischerweise durch ein Drei-Personen-Verhältnis gekennzeichnet ist, besondere Bedeutung. Der Cloud-Nutzer verarbeitet häufig personenbezogene Daten Dritter, etwa von Kunden oder von Mitarbeitern. Der Cloud-Anbieter wirkt als technischer Dienstleister an der Speicherung und der Verarbeitung dieser Daten mit und betreibt damit ebenfalls eine Verarbeitung dieser Daten.[1] In diesem Dreiecksverhältnis besteht besonderer Schutzbedarf, da Rechtsbeziehungen zwar zwischen Cloud-Anbieter und Cloud-Nutzer und häufig auch zwischen Cloud-Nutzer und dem Betroffenen bestehen, Betroffener und Cloud-Anbieter jedoch nicht in vertraglichen Beziehungen zueinander stehen.

Das Datenschutzrecht fängt diese Konstellation traditionell mit dem Instrument der Auftragsverarbeitung[2] auf, das zu Recht die zentrale datenschutzrechtliche Grundlage für Cloud-Dienste darstellt.[3] Bei der Auftragsverarbeitung wird die Weitergabe der Daten an den Dienstleister unter der Voraussetzung zugelassen, dass der Auftraggeber die Kontrolle über die beim Auftragnehmer erfolgende Datenverarbeitung hat und für diese rechtlich verantwortlich ist.

2.2. Herausforderungen der Auftragsverarbeitung im Cloud Computing

Angesichts des beschriebenen Dreiecksverhältnisses gelten in der Auftragsverarbeitung besondere Regeln zum Schutz von Daten gegen unbefugten Zugriff. So sind sowohl der Verantwortliche als auch der Auftragsverarbeiter verpflichtet, angemessene technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau bei der Datenverarbeitung zu gewährleisten (Art. 32 Abs. 1 DSGVO).

Darüber hinaus ist der Verantwortliche als Auftraggeber nach Art. 28 Abs. 1 DSGVO verpflichtet, nur einen solchen Auftragsverarbeiter einzusetzen, der hinreichende Garantien dafür bietet, dass die Anforderungen der DSGVO an die technischen und organisatorischen Maßnahmen erfüllt werden.

Im Ergebnis dürfte dies jedenfalls weitgehend Art. 17 Abs. 1 Datenschutz-Richtlinie entsprechen. Zwar sind die Regelungsschemata unterschiedlich: Art. 17 Datenschutz-Richtlinie erwähnt in Abs. 1 nur den Verantwortlichen als Adressaten der Pflicht zur Datensicherheit, macht aber in Abs. 2 klar, dass sich die Pflicht bei der Auftragsverarbeitung auf die Auswahl des Auftragsverarbeiters und eine Vergewisserung von der Vornahme der nach Abs. 1 geschuldeten Pflichten durch den Auftragsverarbeiter beschränkt. Dasselbe muss auch im Rahmen der DSGVO gelten, da der Verantwortliche seine eigene Pflicht nach Art. 32 Abs. 1 DSGVO nur dadurch erfüllen kann, dass er einen vertrauenswürdigen Auftragsverarbeiter auswählt und sich von der Einhaltung der geschuldeten Maßnahmen überzeugt.

In Deutschland sind die entsprechenden Pflichten des Verantwortlichen in § 11 Abs. 2 BDSG geregelt. Gemäß § 11 Abs. 2 S. 1 BDSG hat der Verantwortliche den Auftragsverarbeiter sorgfältig auszuwählen. Nach § 11 Abs. 2 S. 4 BDSG hat er sich regelmäßig von der Ordnungsgemäßheit der vom Auftragsverarbeiter getroffenen

---

1 Borges/Brennscheidt, in: Borges/Schwenk (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, 2012, S. 43, 62; implizit auch Borges, in: Borges/Meents (Hrsg.), Cloud Computing, Rechtshandbuch, 2016, § 8 Rn. 40, 42.

2 Das BDSG verwendet – synonym – den Begriff der «Auftragsdatenverarbeitung».

3 Borges, in Borges/Meents (Fn. 1.), § 7 Rn. 1; ders., «Kooperation in der IT-Regulierung durch Zertifizierung», in: Schweighofer/Kummer/Hötzendorfer (Hrsg.), Kooperation/Co-Operation, Tagungsband des 18. Internationalen Rechtsinformatik Symposions IRIS 2015, S. 530; Gola/Klug/Körffer, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl. 2015, § 11 Rn. 8; Kompetenzzentrum Trusted Cloud, Arbeitsgruppe «Rechstrahmen des Cloud Computing», Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, S. 5, These 2 S. 7 ff., abrufbar unter: http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/Trusted-Cloud/trustedcloud-ap1-datenschutzrechtliche-loesungen.pdf; Petri, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl. 2014, § 11 Rn. 30; Weichert, DuD 2010, 679, 682 f.

technischen und organisatorischen Maßnahmen zu überzeugen. Dies schließt nach h. M. grundsätzlich auch eine Überprüfung der technischen Maßnahmen des Auftragsverarbeiters vor Ort ein.[4]

Eine so verstandende Überprüfungspflicht ist beim Cloud Computing, dessen Wesen in der gemeinsamen Nutzung durch viele Auftraggeber besteht, problematisch. Für viele Auftraggeber ist sie ohne Inanspruchnahme externer Dienstleister nicht möglich.[5] Vor allem aber ist sie ineffizient, da eine Vielzahl von Cloud-Nutzern denselben Cloud-Dienst – konkret: dieselben technischen und organisatorischen Maßnahmen – zu überwachen hätten.[6]

2.3. Effiziente Überwachung durch Zertifizierung

Diese Nachteile werden durch die Zertifizierung von Cloud-Diensten vermieden, bei der statt aller Cloud-Nutzer ein unabhängiger und kompetenter Dritter,[7] der Zertifizierer, die technischen und organisatorischen Maßnahmen des Cloud-Anbieters überprüft und das Ergebnis der Überprüfung in seinem Zertifikat bestätigt.[8] Auf ein solches Zertifikat sollten Cloud-Nutzer vertrauen dürfen, sofern das Zertifikat und die vorangegangene Prüfung der geschuldeten eigenen Überprüfung entsprechen.[9]

Die datenschutzrechtliche Prüfung und Zertifizierung wird daher zu Recht als Lösung dieses Problems angesehen.[10] Der prominenteste deutsche Ansatz für eine solche Zertifizierung ist die Datenschutz-Zertifizierung nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP).

3. Die Datenschutz-Zertifizierung nach TCDP

3.1. Herausforderungen einer Compliance-Zertifizierung

Prüfung und Zertifizierung von Cloud-Diensten sind nicht neu, ebensowenig die Berücksichtigung von Datenschutz-Aspekten im Rahmen von Zertifizierungen. Es existiert eine Reihe von Gütesiegeln bzw. Zertifikaten für Datenschutz,[11] ebenso etliche Zertifizierungen für Cloud-Dienste.[12]

---

4 Borges, DuD 2014, 165; ders., in: Bundesamt für Sicherheit in der Informationstechnik (BSI), Informationssicherheit stärken – Vertrauen in die Zukunft schaffen. Tagungsband zum 13. Deutschen IT-Sicherheitskongress, 2013, S. 16; Borges/Brennscheidt, in: Borges/Schwenk (Fn. 1), S. 43, 65; Kompetenzzentrum Trusted Cloud (Fn. 3), S. 8. Wohl auch Bergmann/Möhrle/Herb, BDSG, 50. EL 2016, § 11 Rn. 48a; Petri, in: Simitis (Fn. 3), § 11 Rn. 59; Wedde, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 5. Aufl. 2016, § 11 Rn. 57; a.A. Gola/Klug/Körffer, in: Gola/Schomerus (Fn. 3), § 11 Rn. 20.

5 Borges, DuD 2014, 165, 166; Gola/Klug/Körffer, in Gola/Schomerus (Fn. 3), § 11 Rn. 21; Kompetenzzentrum Trusted Cloud (Fn. 3), S. 9; Schuster/Reichl, CR 2010, 38, 42; Selzer, DuD 2013, 215, 216.

6 Borges, DuD 2014, 165, 166; ders., in: Schweighofer/Kummer/Hötzendorfer (Fn. 3), S. 529, 531; ders., in: BSI (Fn. 4), S. 19; Golland, DSB 2014, 213; Kompetenzzentrum Trusted Cloud (Fn. 3), S. 9.; vgl. auch Bergmann/Möhrle/Herb (Fn. 4), § 11 Rn. 48b.

7 Prüfung und Zertifizierung sind regelmäßig zwei Rollen, die durch unterschiedliche Institutionen wahrgenommen werden. Siehe dazu auch unten 3.4.

8 Bergmann/Möhrle/Herb (Fn. 4), § 11 Rn. 48b; Borges, DuD 2014, 165, 166; ders., in: BSI (Fn. 4), S. 19 f.; Borges/Brennscheidt, in: Borges/Schwenk (Fn. 1), 67; Kompetenzzentrum Trusted Cloud (Fn. 3), These 5 S. 12.

9 Kompetenzzentrum Trusted Cloud (Fn. 3), S. 12 ff.; Selzer, DuD 2013, 215, 219; Borges, in: BSI (Fn. 4), S. 19 f.; ders., in: Borges/Meents (Fn. 1), § 7 Rn. 83.

10 Bergmann/Möhrle/Herb (Fn. 4), § 11 Rn. 48b; Borges, DuD 2014, 165, 166; Heckmann, in: Hill/Schliesky (Hrsg.), Innovationen im und durch Recht, 2010, S. 107; Hennrich, CR 2011, 546, 552; Borges/Brennscheidt, in: Borges/Schwenk (Fn. 1), S. 43, 67; Marnau/Schirmer/Schlehan/Schunter, DuD 2011, 333, 336; Schröder/Haag, ZD 2011, 147, 149; Selzer, DuD 2013, 215, 218 f.; Weichert, DuD 2010, 679, 683.

11 Die Stiftung Datenschutz zählt in ihrer – beispielhaften, nicht vollständigen – Übersicht mehr als 30 Gütesiegel und Zertifikate im Bereich Datenschutz auf; die Übersicht ist abrufbar unter https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/SDS-Zertifizierungsuebersicht-November_2016.pdf.

12 Siehe die Übersicht «Cloud-Standards und Zertifizierungen im Überblick» des Kompetenznetzwerks Trusted Cloud e.V., abrufbar unter https://www.trusted-cloud.de/sites/default/files/beitrag-cloud-standards_und_zertifizierungen_im_ueberblick.pdf; siehe ferner die Darstellung ausgewählter Zertifizierungen mit Aussagekraft für die Einhaltung datenschutzrechtlicher Vorgaben von Borges, in: Borges/Meents (Fn. 1), § 7 Rn. 78 ff.

Eine sogenannte «Compliance-Zertifizierung»[13], die die Erfüllung konkreter gesetzlicher Anforderungen bestätigt, hat jedoch spezifische Vorgaben zu erfüllen: Insbesonderes muss sichergestellt sein, dass Prüfung und Zertifizierung die gesetzlichen Anforderungen abbilden und dass die Prüfanforderungen einheitlich und transparent sind (dazu sogleich 3.3.). Ferner ist sicherzustellen, dass das Verfahren der Prüfung und Zertifizierung den Anforderungen einer ordnungsgemäßen Zertifizierung entspricht, insbesondere müssen Prüfer und Zertifizierer unabhängig und fachlich kompetent sein (dazu unten 3.4.).[14]

Die Zertifizierung nach dem TCDP nimmt für sich in Anspruch, diese Anforderungen zu erfüllen. Die wesentlichen Elemente dieser Zertifizierung werden nachfolgend dargestellt.

3.2. Trusted Cloud und Pilotprojekt «Datenschutz-Zertifizierung für Cloud-Dienste»

Die Datenschutz-Zertifizierung nach dem TCDP geht auf das von 2011–2015 durchgeführte Technologieprogramm «Trusted Cloud» des BMWi zurück, in dem 14 ausgewählte Cloud-Projekte gefördert wurden.[15] Im Rahmen der für Technologieprogramme üblichen Begleitforschung wurden zugleich die Rahmenbedingungen für die weitere Entwicklung des Cloud Computing untersucht.

Die Aktivitäten zu den rechtlichen Rahmenbedingungen des Cloud Computing wurden in der vom Verfasser geleiteten und mit Vertretern aller maßgeblichen Stakeholder besetzten Arbeitsgruppe «Rechtsrahmen des Cloud Computing» zusammengefasst,[16] deren Arbeitsergebnisse in einer Reihe von Papieren veröffentlicht wurden.[17] Ein wesentliches Arbeitsergebnis stellt das Konzeptpapier «Datenschutzrechtliche Lösungen für Cloud Computing» von Oktober 2012 dar, in dem wesentliche Merkmale einer Datenschutz-Zertifizierung für Cloud-Dienste beschrieben wurden.[18]

Im Pilotprojekt «Datenschutz-Zzuertifizierung für Cloud-Dienste», an dem Vertreter der maßgeblichen Stakeholder, darunter insgesamt 7 Datenschutzbehörden, mitwirkten,[19] wurden die wesentlichen Grundlagen einer Datenschutz-Zertifizierung entwickelt. Dazu gehört insbesondere ein Datenschutzstandard, das «Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)», das zunächst in einer Version 0.9 im April 2015 veröffentlicht[20] und sodann, auf der Grundlage einer Pilot-Zertifizierung und einer öffentlichen Anhörung, zur Vollversion TCDP 1.0 weiterentwickelt wurde.[21] Daneben entstanden im Rahmen des Pilotprojekts eine Verfahrensordnung für Zertifizierungen nach dem TCDP[22] sowie eine Reihe begleitender Papiere.[23]

3.3. Abbildung gesetzlicher Datenschutzanforderungen durch einen Prüfstandard

Die zentrale Aufgabe des TCDP ist es, die gesetzlichen Anforderungen an die Auftragsdatenverarbeitung, die Gegenstand der Überprüfung durch den Cloud-Nutzer nach § 11 Abs. 2 S. 4 BDSG sind, in einen prüffähigen

---

13 Der Begriff wird zur Abgrenzung gegenüber unspezifischen Gütesiegeln vewendet in: Kompetenzzentrum Trusted Cloud, Pilotprojekt «Datenschutz-Zertifizierung für Cloud-Dienste», Nr. 12, «Thesenpapier – Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste», S. 8.

14 Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Cloud Computing, Version 2.0, Ziff. 3, S. 10; Borges in: Borges/Meents (Fn. 1), § 7 Rn. 86; Kompetenzzentrum Trusted Cloud (Fn. 3), S. 13; Weichert, DuD 2010, 679, 683.

15 http://www.digitale-technologien.de/DT/Navigation/DE/Service/Abgelaufene_Programme/Trusted-Cloud/trusted-cloud.html.

16 Kompetenzzentrum Trusted Cloud (Fn. 3), S. 3.

17 Die Ergebnispapiere sind abrufbar unter: http://www.digitale-technologien.de/DT/Navigation/DE/Service/Abgelaufene_Programme/Trusted-Cloud/Rechtsrahmen/rechtsrahmen.html.

18 Kompetenzzentrum Trusted Cloud (Fn. 3).

19 Vgl. etwa Liste der Beteiligten in Kompetenzzentrum Trusted Cloud (Fn. 13), S. 22.

20 Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) – Version 0.9, abrufbar unter: http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/Trusted-Cloud/trustedcloud-datenschutzprofil-tcdp.pdf.

21 Trusted Cloud-Datenschutzprofil für Cloud-Dienste – Version 1.0, abrufbar unter: http://tcdp.de/data/pdf/TCDP-1-0.pdf.

22 Verfahrensordnung für Zertifizierungen nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP), abrufbar unter: http://tcdp.de/data/pdf/Verfahrensordnung-1-0.pdf.

23 Siehe dazu die Übersicht der veröffentlichten Begleitpapiere, abrufbar unter http://tcdp.de/index.php/start.

Standard umzusetzen.[24] Entsprechend geht das TCDP von den gesetzlichen Anforderungen aus. Eine Normentabelle, die Bestandteil des Standards ist, stellt im Einzelnen dar, welche Normen des BDSG berücksichtigt und in welchen Normen des TCDP sie jeweils umgesetzt werden.[25] Damit bringt das TCDP einen wesentlichen Fortschritt gegenüber den meisten bisherigen Standards, die häufig zwar datenschutzrechtliche Aspekte berücksichtigen, aber keine genaue Umsetzung des BDSG leisten.[26] Ein insoweit ähnlicher Ansatz wird aber beispielweise im Standard «DS-BvD-GDD-01»[27] verfolgt.[28]

Eine zentrale Herausforderung ist die Sicherung von Einheitlichkeit und Transparenz der Prüfanforderungen. In der Vergangenheit wurden von Unternehmen, die eine datenschutzrechtliche Prüfung und Zertifizierung anboten, notgedrungen eigene Standards verwendet, die jeweils nur innerhalb des Unternehmens oder einer Unternehmensgruppe verwendet wurden. Damit war die Einheitlichkeit der Prüfanforderungen aber nicht gewährleistet. Weiterhin waren die eigenen Standards nicht veröffentlicht. Damit ist es weder für Dritte, wie Aufsichtsbehörden, möglich zu überprüfen, ob der Standard die gesetzlichen Anforderungen korrekt umsetzt, noch ist es für mögliche Interessenten einer Zertifizierung möglich, vorab festzustellen, welche konkreten Anforderungen im Rahmen der Prüfung und Zertifizierung einzuhalten sind.

Entsprechend ist es das vorrangige Ziel des TCDP, einen einheitlichen und transparenten Standard zu schaffen. Dieses Ziel wird dadurch erreicht, dass das TCDP öffentlich und für jedermann kostenfrei nutzbar ist. Dabei ist entscheidend, dass die Konkretisierung der Prüfanforderungen wiederrum durch transparente und einheitliche Kriterien erfolgt. Insoweit macht sich das TCDP die Arbeiten der ISO-Standards zu Nutze, konkret der ISO 27000-Gruppe und insbesondere der Standards ISO/IEC 27018[29] und ISO/IEC 27002[30].[31]

Die Einbeziehung der ISO-Standards hat mehrere zentrale Vorteile: Die ISO 27000-Gruppe ist weltweit bekannt und eine wesentliche Richtschnur für die Praxis in vielen Staaten.[32] Besonders vorteilhaft ist, dass die ISO mit dem 2014 veröffentlichten Standard ISO/IEC 27018 einen Standard entwickelt hat, dessen Ziel es ist, zentrale Anforderungen der Europäischen Datenschutz-Richtlinie umzusetzen.[33] Die Zielsetzung von ISO/IEC 27018 ist also ganz ähnlich, wie die des TCDP.

Das TCDP verweist auf ISO/IEC 27018 und auf ISO/IEC 27002, soweit diese geeignet sind, die Anforderungen des BDSG zu konkretisieren, und enthält darüber hinaus eigene Anforderungen oder weicht von den ISO-

24 Vgl. TCDP – Version 1.0 (Fn. 21), S. 4; sowie schon TCDP – Version 0.9 (Fn. 20), S. 4 f.

25 TCDP – Version 1.0 (Fn. 21), S. 10 f.

26 Vgl. zur fehlenden Aussagekraft einzelner Gütesiegel und Zertifizierungen mit Einzelnachweisen Borges, in: Borges/Meents (Fn. 1), § 7 Rn. 79 ff.; speziell zu ISO/IEC 27001 auch Kraska, ZD 2016, S. 153.

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

28 Staub, DuD 2014, 159, 160.

29 DIN ISO/IEC 27018 Informationstechnik – Sicherheitsverfahren – Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2014).

30 DIN ISO/IEC 27002 Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Maßnahmen (ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015).

31 TCDP – Version 1.0 (Fn. 21), S. 4.

32 Borges, in: Schweighofer/Kummer/Hötzendorfer (Fn. 3), S. 533; vgl. ferner Conrad, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 33 Rn. 306 ff.; Schmidl, in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl. 2016, § 28 Rn. 126 f.; speziell zur ISO 27001 Foitzick/Plankemann, CCZ 2015, 180, 183; ähnlich Kraska, ZD 2016, 153, der ISO 27001 als die derzeit vielversprechendste Norm für einen international anerkannten Standard bezeichnet.

33 Borges, in: Borges/Meents (Fn. 1), § 7 Rn 81.

Normen ab, soweit dies geboten ist.[34] Außerdem bezieht das TCDP in der 2016 veröffentlichten Version den Standard ISO/IEC 27017[35] zur IT-Sicherheit für Cloud-Dienste ein.[36]

Die genannten ISO-Standards unterscheiden sich vom TCDP entscheidend insoweit, als ihre Normen keine Prüfanforderungen darstellen, sondern im Rahmen anderer Prüfungen, insbesondere nach ISO/IEC 27001, verwendet werden. Im Rahmen einer ISO/IEC 27001-Prüfung wird der Prüfumfang zwischen den Parteien individuell vereinbart. In diesem Aspekt ist das TCDP aufgrund seiner spezifischen Zielsetzung, gesetzliche Anforderungen umzusetzen, wesentlich anders: Die Normen des TCDP verstehen sich sämtlich als verbindliche Elemente einer Prüfung, Abweichungen von den TCDP-Normen sind nicht möglich. Die etwa in ISO/IEC 27002 als «control» genannten Normen, werden im TCDP damit grundsätzlich zu verbindlichen Anforderungen.[37]

Mit dieser Verweisstruktur des TCDP wird eine transparente Konkretisierung der gesetzlichen Anforderungen erreicht, die bisher kein anderer Standard zur datenschutzrechtlichen Prüfung von Cloud-Diensten oder Auftragsverarbeitung aufweisen kann.

3.4. Die Verfahrensordnung für Zertifizierungen nach TCDP

Für eine verlässliche Zertifizierung ist das Verfahren der Zertifizierung von entscheidender Bedeutung. Das Zertifikat ist nur verlässlich, wenn sowohl eine ordnungsgemäße Prüfung als auch eine ordnungsgemäße Zertifizierung gesichert sind. Daher hat das Pilotprojekt eine Verfahrensordnung für Zertifizierungen nach dem TCDP ausgearbeitet, die gleichzeitig mit TCDP 1.0 im September 2016 veröffentlicht wurde.[38]

Die Verfahrensordnung, die in deutscher, englischer und französischer Sprache verfügbar ist, enthält in sechs Kapiteln mit insgesamt 35 Paragraphen sowie 2 Anlagen eine umfangreiche Regelung der Prüfung und Zertifizierung von Cloud-Diensten nach dem TCDP.[39]

Das kurze erste Kapitel regelt entsprechend seinem Titel «Anwendungsbereich» insbesondere den Zusammenhang der Verfahrensordnung mit dem TCDP 1.0. Große Bedeutung hat das zweite Kapitel «Zertifizierungsstelle und Prüfstelle», das eine wesentliche Grundentscheidung für das Zertifizierungsverfahren trifft, indem es ausdrücklich zwischen der Prüfstelle und der Zertifizierungsstelle unterscheidet und damit den unterschiedlichen Aufgaben der Prüfung und Zertifizierung zwei unterschiedliche Rollen im Zertifizierungsverfahren zuweist. Zudem wird ausdrücklich bestimmt, das Prüfung und Zertifizierung voneinander unabhängig zu erfolgen haben (§ 2.6 Abs. 1 Verfahrensordnung). Das Kapitel regelt insbesondere die Anforderungen an die Prüfstelle und die Zertifizierungsstelle, namentlich die fachliche Eignung und Unabhängigkeit der beiden Stellen, die durch eine Akkreditierung nachzuweisen ist (vgl. § 2.5 Verfahrensordnung).

Das dritte Kapitel regelt das Verfahren der Prüfung. Die Möglichkeit der Anerkennung von Zertifikaten mit der Wirkung, dass im Umfang des Zertifikats eine Prüfung des im Zertifikat benannten Bestandteils des Cloud-Dienstes nicht erforderlich ist, ist in § 3.4 ausdrücklich geregelt. Die Verfahrensordnung regelt hier auch ausdrücklich eine Zwischenprüfung, die turnusmäßig oder bei Änderungen des Cloud-Dienstes erforderlich ist (§ 3.6).

Das vierte Kapitel enthält die Regelung zum eigentlichen Zertifizierungsverfahren. Hier sind unter anderem die Voraussetzungen der Anerkennung von TCDP-Zertifikaten (§ 4.4) sowie von anderen Zertifikaten (§ 4.5)

---

34 Vgl. TCDP – Version 1.0 (Fn. 21), S. 5 f.

35 ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

36 TCDP – Version 1.0 (Fn. 21), S. 4 f.

37 TCDP – Version 1.0 (Fn. 21), S. 5 f.

38 TCDP Version 1.0 veröffentlicht, Meldung vom 4. Oktober 2016, auf der Webseite des TCDP, abrufbar unter: http://tcdp.de/index.php/aktuelles/14-tcdp-version-1-0-veroeffentlicht.

39 Verfahrensordnung TCDP (Fn. 22).

im Einzelnen geregelt. Detailliert geregelt sind auch die möglichen Entscheidungen der Zertifizierungsstelle (§ 4.6) sowie die Möglichkeit eines Widerspruchs des Cloud-Anbieters gegen eine nachteilige Entscheidung (§ 4.8). Durch eine sogenannte «Änderungszertifizierung» (§ 4.9) wird die Möglichkeit eingeräumt, bei Änderungen des Cloud-Dienstes eine Änderung des Zertifikats durch ein verkürztes Zertifizierungsverfahren zu erreichen.

Das Zertifikat ist im fünften Kapitel im Einzelnen geregelt. Der Inhalt des Zertifikats wird in § 5.1 detailliert beschrieben, ein Zertifikatsmuster (Anlage 1 der Verfahrensordnung) erleichtert die Erfüllung der Anforderungen. Das Zertifikat ist von der Zertifizierungsstelle zu veröffentlichen (§ 5.2). Das Zertifikat wird gemäß § 5.3 für eine Zeit von längstens drei Jahren ausgestellt, während der Laufzeit ist eine «Überwachung» (§ 5.4) in Form jährlicher Zwischenprüfungen erforderlich. Die Erteilung des Zertifikats berechtigt den Cloud-Anbieter, das TCDP-Prüfzeichen (Anlage 2) zu führen.

Das fünfte Kapitel enthält schließlich eine detaillierte Regelung zu Einschränkung, Aussetzung oder Widerruf des Zertifikats (§ 5.6). Insbesondere wird die Zertifizierungsstelle verpflichtet, das Zertifikat zu widerrufen, wenn sie feststellt, dass die Voraussetzungen für dessen Erteilung nicht vorlagen oder nicht mehr vorliegen. Eine solche Maßnahme kann freilich nicht ohne vorherige Anhörung des Cloud-Anbieters erfolgen (§ 5.6 Abs. 6 S. 2).

Im abschließenden sechsten Kapitel drücken die Beteiligten des Pilotprojekts als Verfasser der Verfahrensordnung die Erwartung aus, dass die Zertifizierung nach dem TCDP zu einer Zertifizierung auf der Grundlage der DSGVO fortentwickelt wird und dass TCDP-Zertifikate auf ein Zertifikat nach DSGVO übertragen werden können (§ 6.1 Abs. 2). Eine entsprechende Übergangsregelung ist vorbereitet (§ 6.1 Abs. 3).

4. Die Regelung der DSGVO zur Datenschutz-Zertifizierung

4.1. Grundsätze der Datenschutz-Zertifizierung

Die DSGVO ist dem Konzept der Datenschutz-Zertifizierung, das dem TCDP zugrunde liegt, freundlich gesonnen: Anders als die Datenschutz-Richtlinie enthält die DSGVO in ihren Artt. 42 f. eine recht umfassende, gesetzliche Regelung zur Zertifizierung.

Art. 42 Abs. 1 verpflichtet die Mitgliedstaaten, die Entwicklung von Datenschutz-Zertifizierungen zu fördern. Interessant ist, dass die Zertifizierung gemäß Art. 42 Abs. 2 auch im Rahmen der Übertragung von Diensten in Drittstaaten genutzt werden kann, konkret, um das Vorliegen hinreichender Garantien nachzuweisen. Dies ist eine wesentliche Erweiterung der Möglichkeiten der Datenschutz-Zertifizierung.[40]

Art. 42 enthält in den Absätzen 3–7 einige wesentliche Grundsätze für Zertifizierungsverfahren. Diese müssen freiwillig sein (Abs. 3) und können die Befugnisse der Datenschutzaufsicht nicht beschränken (Abs. 4). Zertifikate können durch spezielle Zertifizierungsstellen oder durch die Aufsichtsbehörden erteilt werden (Abs. 5). Der Antragsteller muss der Zertifizierungsstelle alle erforderlichen Informationen zur Verfügung stellen (Abs. 6). Das Zertifikat wird für eine Höchstdauer von 3 Jahren erteilt und kann verlängert werden (Abs. 7, S. 1). Das Zertifikat ist zu widerrufen, wenn die Voraussetzungen für die Erteilung nicht mehr vorliegen (Abs. 7, S. 2).

4.2. Compliance-Zertifizierung für Auftragsverarbeitung

Die Regelung des Art. 42 DSGVO ist recht allgemein gehalten. Der Begriff der Zertifizierung ist sehr umfassend und umfasst alle Arten von Gütesiegeln und Zertifikaten. Die DSGVO ermöglicht aber auch eine Compliance-Zertifizierung für Auftragsverarbeiter nach dem Konzept des TCDP. Dies ergibt sich aus der Regelung der Auftragsverarbeitung in Art. 28 DSGVO. Gemäß Art. 28 Abs. 1 DSGVO darf der Verantwortliche

[40] Vgl. Spindler, ZD 2016, 407, 410.

nur solche Auftragsverarbeiter beauftragen, die hinreichende Garantien für die Durchführung geeigneter technischer und organisatorischer Maßnahmen bieten.

Entscheidende Voraussetzung für eine gesetzeskonforme Auftragsverarbeitung ist damit das Vorliegen der entsprechenden «hinreichenden Garantien». Insoweit enthält Art. 28 Abs. 5 DSGVO eine entscheidende Neuerung gegenüber der Datenschutz-Richtlinie. Danach kann die Einhaltung von Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 «als Faktor herangezogen werden», um hinreichende Garantien nachzuweisen.

Da diese Formulierung recht vage ist, ist unklar, welche Bedeutung der Zertifizierung insoweit zukommt. Dies dürfte dem Umstand geschuldet sein, dass die Begriffe der «Verhaltensregeln» und der «Zertifizierung» eine Vielzahl ganz unterschiedlicher Konzepte und Regeln zur Zertifizierung umfassen, denen folglich auch unterschiedliche rechtliche Bedeutung zukommen muss. Unstreitig ist, dass die Zertifizierung keine Bindung der Aufsichtsbehörden bewirkt, wie sich aus Art. 42 Abs. 4 DSGVO ergibt,[41] und ebenso nicht den vollen Nachweis der Erfüllung der Anforderungen erbringt,[42] also auch Gerichte nicht bindet.

Teilweise wird angenommen, dass mit der Genehmigung eines Zertifizierungsverfahrens eine Selbstbindung der Verwaltung eintrete.[43] Allerdings bleibt unklar, wie weit diese Selbstbindung reichen soll. Unstreitig dürfte wiederum sein, dass im Rahmen von Art. 28 Abs. 5 DSGVO die Aufsichtsbehörden nicht frei darin sind, Zertifizierungen zu ignorieren. So wird man annehmen können, dass den Aufsichtsbehörden hinsichtlich des «Ob» der Berücksichtigung der Zertifizierung ein intendiertes Entschließungsermessen eingeräumt wird,[44] mit der Folge, dass die Zertifizierung jedenfalls als Indiz herangezogen werden muss, soweit nicht begründete Zweifel daran bestehen, dass das eingesetzte Zertifikat hierzu völlig ungeeignet ist. Welches Gewicht die Aufsichtsbehörde dem Zertifikat im Rahmen des Abwägungsvorgangs beizumessen hat, ist freilich nicht konkret vorgegeben. Dieses muss vielmehr von der Qualität des Zertifikats, namentlich von seinen materiellen Grundlagen (Prüfkriterien) sowie der Ausgestaltung des Zertifizierungsverfahrens abhängen.

Je mehr nun das Zertifikat und das zugrundeliegende Verfahren geeignet sind, das Vorliegen hinreichender Garantien nachzuweisen, desto stärkeres Gewicht muss dem Zertifikat im Rahmen der Beurteilung zukommen.

Im Fall einer Zertifizierung nach dem Muster des TCDP, das auf einer Prüfung der gesetzlichen Anforderungen beruht, dürfte sich die Wirkung dahin verdichten, dass die Einsichtnahme in das Zertifikat zur Vergewisserung über das Vorliegen geeigneter Garantien im Sinne von Art. 28 Abs. 1 DSGVO ausreicht und somit der Cloud-Nutzer befugt ist, den Dienst des zertifizierten Cloud-Anbieters zu nutzen.

4.3. Anforderungen an das Zertifizierungsverfahren

Art. 43 DSGVO enthält weitere Anforderungen an Zertifizierungsstellen sowie an das Zertifizierungsverfahren. Nach Art. 43 Abs. 1 sind Zertifizierungsstellen zu akkreditieren. Ob die Akkreditierung durch Aufsichtsbehörden oder durch die nationale Akkreditierungsstelle durchgeführt wird, überlässt die DSGVO den Mitgliedstaaten. Wesentliche Anforderungen an die Zertifizierungsstellen sind deren Unabhängigkeit und fachliche Kompetenz (vgl. Art. 43 Abs. 2 DSGVO). Zertifizierungsstellen sind für die ordnungsgemäße Durchführung der Zertifizierung verantwortlich (Art. 43 Abs. 4 DSGVO).

5. Perspektiven der Datenschutz-Zertifizierung in der DSGVO

5.1. TCDP-Zertifizierung und DSGVO

Das Grundanliegen der TCDP-Zertifizierung, die Überwachungspflicht des Nutzers von Cloud-Diensten durch eine genehmigte Zertifizierung entscheidend zu erleichtern, findet seine gesetzliche Grundlage in Art. 28

41 Spindler, ZD 2016, 407, 410.
42 Plath, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2016, Art. 18 Rn. 15.
43 Spindler, ZD 2016, 407, 412.
44 Martini, in: Paal/Pauly (Hrsg.), DSGVO, 2017, Art. 28 Rn. 69.

Abs. 5 DSGVO. Entscheidende Voraussetzung für den Effekt des Art. 28 Abs. 5 DSGVO ist die «Genehmigung» des Zertifizierungsverfahrens nach Art. 42 DSGVO. Voraussetzung und Verfahren der Genehmigung sind freilich nicht klar geregelt. Insoweit wird sich eine Praxis erst noch herausbilden müssen.

Eine zentrale Anforderung für eine Datenschutz-Zertifizierung auf der Grundlage der DSGVO nach dem Konzept des TCDP ist die Existenz eines auf die materiellen Anforderungen der DSGVO zugeschnittenen Prüfstandards. Ein solcher Standard existiert bisher nicht. TCDP 1.0 beruht nicht auf der DSGVO, ebenso wenig gibt es – soweit ersichtlich – einen anderen Standard, der explizit die Anforderungen der DSGVO implementiert.

Dies schließt die Annahme nicht aus, dass TCDP 1.0 oder ein anderer Standard, etwa ISO/IEC 27018, als Umsetzung der Anforderungen der DSGVO an die technischen und organisatorischen Maßnahmen angesehen werden, zumal die Regeln der DSGVO insoweit rudimentär sind und eine Konkretisierung der Anforderungen fehlt. Vorzugswürdig gegenüber einer solchen Anerkennung bestehender Standards, die sich an der Datenschutz-Richtlinie orientieren, ist freilich die Entwicklung eines neuen Standards, der die Anforderungen der DSGVO möglichst präzise abbildet.

Das Verfahren der TCDP-Zertifizierung berücksichtigt bereits die Anforderungen der DSGVO. Freilich sind die Regeln der DSGVO zum Verfahren ausfüllungsbedürftig, sodass sich Änderungen ergeben können.

5.2. Offene Fragen der Datenschutz-Zertifizierung nach DSGVO

Es gibt eine Reihe offener Fragen im Zusammenhang mit der Datenschutz-Zertifizierung nach der DSGVO. So ist noch recht unklar, welche Vorgaben hinsichtlich der materiellen Prüfanforderungen gelten sollen.

Die DSGVO gibt der Kommission weitreichende Möglichkeiten, die Anforderungen an Zertifizierungen zu präzisieren. Gemäß Art. 43 Abs. 8 DSGVO kann sie Anforderungen an Zertifizierungsverfahren regeln. Darüber hinaus kann sie nach Art. 43 Abs. 9 DSGVO technische Standards sowie Mechanismen zur Anerkennung von Zertifizierungsverfahren festlegen. In der Literatur wird teilweise aus Gründen der Rechtssicherheit ein rasches Tätigwerden der Kommission befürwortet.[45] Ob die Kommission von dieser Befugnis Gebrauch machen wird, ist derzeit noch unklar.[46]

Ferner ist noch weitgehend unklar, welche Voraussetzungen der Datenschutz-Ausschuss an die Genehmigung nach Art. 42 DSGVO stellen wird. Insoweit kann derzeit keine Vorhersage getroffen werden. Die Praxis wird daher sehr genau beobachten, welche Signale der Ausschuss insoweit sendet.

Schließlich bestehen offene Fragen in Bezug auf das Grundanliegen der Zertifizierung für Cloud-Dienste, die Erleichterung der Überwachungspflicht der Cloud-Nutzer. Es ist anzunehmen, dass Zertifizierungsverfahren mit ganz unterschiedlichen Zielen und Inhalten den Status eines Europäischen Datenschutz-Gütesiegels anstreben werden. Es ist jedoch noch sehr offen, welche Bedeutung den verschiedenen Verfahren gemäß Art. 28 Abs. 5 DSGVO in Bezug auf die Pflicht zur Auswahl des Auftragsverarbeiters nach Art. 28 Abs. 1 DSGVO zukommen wird. Diese Frage werden vorerst die Aufsichtsbehörden und vor allem die Gerichte zu beantworten haben, da zweifelhaft ist, ob sich die Konkretisierungsbefugnis der Kommission im Hinblick auf die Anerkennung von Zertifizierungsverfahren nach Art. 43 Abs. 9 DSGVO auch auf die Ausgestaltung der Rechtsfolgen einer Zertifizierung – etwa im Rahmen von Art. 28 Abs. 5 DSGVO – erstreckt.

6. Fazit

Die Datenschutz-Zertifizierung im Sinne einer Compliance-Zertifizierung, die das Vorliegen gesetzlicher Anforderungen bestätigt, ist ein überzeugendes Konzept für die Verbesserung der Datensicherheit. Sie ermöglicht es im Fall der Auftragsverarbeitung, die bei modernen Formen der Datenverarbeitung – insbesondere bei der

---

45 Hofmann, ZD-Aktuell 2016, 05324 (dort 6.).

46 Dies ist derzeit offenbar nicht geplant, vgl. Kipker/Dix, ZD-Aktuell 2016, 04197 unter Verweis auf die Äußerungen von Thomas Zerdick, stellvertretender Leiter des Referats C.3 (Schutz personenbezogener Daten) bei der Generaldirektion Justiz und Verbraucher der Europäischen Kommission.

Nutzung von Cloud-Diensten – den Standardfall der Datenverarbeitung ausmacht, die für die Gewährleistung von Datensicherheit notwendige Überprüfung der Maßnahmen vor Ort in einem effizienten Verfahren durchzuführen und schafft damit die Grundlage für die tatsächliche Durchführung einer technischen Überprüfung durch unabhängige Dritte.

Die Datenschutz-Grundverordnung bringt einen wesentlichen Fortschritt in Bezug auf die Zertifizierung. Sie enthält erstmals eine gesetzliche Regelung zur datenschutzrechtlichen Zertifizierung, und sie öffnet die Tür, um der Zertifizierung in vielfacher Hinsicht rechtliche Bedeutung beizumessen. Besonders wichtig sind dabei die Wirkungen im Bereich der technischen und organisatorischen Maßnahmen, der Auftragsverarbeitung und der Übertragung von Daten in Drittstaaten. Damit ergeben sich für die Datenschutz-Zeritifizierung erhebliche Chancen.

Freilich sind die Regelungen der DSGVO recht allgemein und bedürfen der Konkretisierung. Für die erforderliche Fortentwicklung der Zertifizierung wird es, neben etwaigen Rechtsakten der EU-Kommission, auf die Haltung der Aufsichtsbehörden, insbesondere im Europäischen Datenschutz-Ausschuss, aber auch auf Initiativen aus Wissenschaft und Praxis ankommen.

Im Bereich der Zertifizierung von Auftragsverarbeitern können die im Pilotprojekt «Datenschutz-Zertifizierung für Cloud-Dienste» erarbeitete Verfahrungsordnung und der Prüfstandard TCDP 1.0 eine taugliche Grundlage für die erforderliche Konkretisierung und Fortentwicklung der Datenschutz-Zertifizierung bilden.