# Cloud-Dienst-Zertifizierungen zur Schaffung von Vertrauen in und Transparenz von digitalen Diensten

*Ali Sunyaev*

## *I. Einleitung*

Cloud-Computing ist eine Weiterentwicklung der Computertechnologie und ein dominierendes Geschäftsmodell für die bedarfsgerechte Bereitstellung von IT-Infrastruktur, Komponenten und Anwendungen als Internet-Dienste.[1] Heutzutage nutzen wir in unserem Alltag bereits (unbewusst) eine immer größere Anzahl und Vielfalt von Cloud-Diensten, zum Beispiel zum Austausch von Nachrichten (z.B. WhatsApp), bei der Zusammenarbeit in Teams (z.B. Asana), dem Management von Unternehmen (z.B. SAP ByDesign) und bei Online-Spielen (z.B. GamingAnywhere). Cloud-Computing stellt u.a. die Infrastruktur bereit, die andere essentielle digitale Trends wie Mobile Computing, das Internet der Dinge, Big Data und künstliche Intelligenz vorangetrieben hat, wodurch innovative Geschäftsmodelle realisiert wurden und die digitale Transformation vorangetrieben wird. Heute ist Cloud-Computing zu einer kritischen IT-Infrastruktur für fast jeden Aspekt unseres täglichen Lebens geworden.

Dieser unvergleichliche Zugang zu IT-Ressourcen hat seinen Preis: Unternehmen haben oft Schwierigkeiten, zuverlässige und sichere digitale Dienste von unzuverlässigen, nicht vertrauenswürdigen zu unterscheiden. Außerdem sind Kunden während der Nutzung dieser Dienste ständigen Sicherheits- und Datenschutzrisiken ausgesetzt, wie die schwerwiegenden Datenschutzverstöße von Unternehmen wie Facebook, Apple, Sony und Adobe zeigen. Folglich müssen Cloud-Anbieter die Sicherheit und den Datenschutz ihrer Dienste gewährleisten und (potenziellen) Cloud-Kunden transparent vermitteln. In diesem Zusammenhang können Zertifizierungen von Cloud-Diensten Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Kundenseite erhöhen sowie es Cloud-Anbietern ermöglichen,

1 *Benlian/Kettinger/Sunyaev/Winkler*, Special Section: The Transformative Value of Cloud Computing, Journal of Management Information Systems 35 (2018), 719, 720 ff.

ihre Systeme und Prozesse zu überprüfen und zu verbessern.[2] Allerdings sind traditionelle Zertifizierungen im Cloud-Computing-Umfeld aufgrund von inhärenter Dynamik und der ständigen (technischen) Weiterentwicklung von Cloud-Diensten kritisch zu betrachten. Um die Glaubwürdigkeit ausgestellter Zertifikate zu erhöhen und um kontinuierlich sicherzustellen, dass Cloud-Dienste sicher und zuverlässig angeboten werden, eignet sich der Einsatz von *kontinuierlichen Zertifizierungen*, welche es ermöglichen, kritische Anforderungen an Cloud-Dienste kontinuierlich und (teil-)automatisiert zu überprüfen.[3] Hierbei muss jedoch der genaue Umfang der Prüfprozesse festgelegt werden, da nicht jedes Zertifizierungskriterium automatisiert prüfbar ist bzw. eine automatisierte Überprüfung fordert. Im Rahmen dieses Beitrags wird daher exemplarisch für Datenschutzzertifizierungen untersucht, ob eine fortlaufende Überprüfung im Sinne einer kontinuierlichen Zertifizierung auch im Themenfeld des Datenschutzes möglich ist. Daher vereint dieser Beitrag zwei Themenschwerpunkte von Alexander Roßnagel, den Datenschutz und die (kontinuierliche) Zertifizierung.

## *II. Grundlagen zur Zertifizierung von Cloud-Diensten*

### *1. Cloud-Dienste*

Cloud-Computing bezeichnet ein IT-Bereitstellungsmodell, welches einen flexiblen und bedarfsorientierten Zugriff auf eine gemeinsam genutzte Sammlung von konfigurierbaren IT-Ressourcen ermöglicht, die über das Internet oder ein Netzwerk abgerufen werden.[4] Darunter fällt bspw. der Zugriff auf Netzwerke, Server, Speicher oder Anwendungen. Die für Cloud-Computing kennzeichnenden Charakteristiken sind insbesondere der bedarfsgerechte Zugriff, die Möglichkeit zur Ressourcenbündelung und eine hohe Skalierbarkeit. So ist es bspw. möglich, je nach aktuellem Bedarf, erhaltene Rechen-, Speicher- oder Bandbreitenkapazitäten zu erhöhen oder zu reduzieren. Unter anderem deshalb entsteht für den Cloud-

2 *Lins/Schneider/Sunyaev*, Cloud-Service-Zertifizierung, 2. Aufl., Berlin 2019, 1 f.
3 *Banse/Stephanow*, Motivation, Bausteine und Vorgehensweise, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 1 ff.
4 *Mell/Grance*, The NIST Definition of Cloud Computing, 2011, 2 f.

Kunden der Eindruck, dass Ressourcen nahezu unbegrenzt und zu jeder Zeit in jedem Ausmaß verfügbar sind.

Im Cloud-Computing kann zwischen drei grundlegenden Dienst- bzw. Service-Modellen, nämlich Software as a Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS), unterschieden werden.[5] Bei SaaS kann der Cloud-Kunde mittels verschiedener Geräte entweder über einen Web-Browser oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen. Bei PaaS kann der Cloud-Kunde selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Anbieters installieren und betreiben. Hierzu werden Programmiersprachen, Programmbibliotheken oder weitere vom Cloud-Anbieter unterstützte Dienste und Werkzeuge genutzt. Bei IaaS erhält der Cloud-Kunde Zugang zu Hardwareressourcen des Cloud-Anbieters, darunter fallen bspw. Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger Software verwenden, bspw. Betriebssysteme oder Anwendungen.

## 2. *Zertifizierung von Cloud-Diensten*

Cloud-Anbieter sehen sich mit vielen Bedenken von potentiellen Cloud-Kunden hinsichtlich des Vertrauens in die angebotenen Dienste und deren Sicherheit konfrontiert.[6] Es zeigt sich, dass Zertifizierungen zur Adressierung dieses Problems beitragen können, indem sie Vertrauen schaffen, die Transparenz im Cloud-Dienst-Markt erhöhen und es Cloud-Anbietern ermöglichen, eingesetzte Systeme und Prozesse zu verbessern.[7] Eine Zertifizierung ist definiert als ein Verfahren, welches durch eine unabhängige dritte Partei durchgeführt wird und formal verifiziert, dass ein Produkt, ein Prozess, ein System oder eine Person zu definierten Kriterien und Anforderungen konform ist.[8] Das schriftliche Ergebnisdokument, welches diese Konformität festhält, wird als Zertifikat bezeichnet. Es gibt heutzutage bereits eine Vielzahl von Zertifizierungen für Cloud-Dienste auf dem

---

5 *Mell/Grance* (Fn. 4), 2 f.

6 *Schneider/Sunyaev*, Determinant factors of cloud-sourcing decisions, Journal of Information Technology 31 (2016), 1, 7 ff.

7 *Sunyaev/Schneider*, Cloud services certification, Commun. ACM 56 (2013), 33, 33 ff.

8 *Lansing/Benlian/Sunyaev*, "Unblackboxing" Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications, Journal of the Association for Information Systems 19 (2018), 1064, 1066.

Markt.[9] So führt bspw. EuroCloud die Zertifizierung „*EuroCloud Star Audit*" durch, indem ein Dokumentenreview und eine Vor-Ort-Auditierung vorgenommen werden.

Cloud-Anbieter können eine Vielzahl von Vorteilen generieren, wenn sie sich einer Zertifizierung unterziehen.[10] Durch ein Zertifikat kann vor allem das Kundenvertrauen in den angebotenen Cloud-Dienst gesteigert werden. Das Zertifikat kann aber auch als ein Marketinginstrument verwendet werden, indem bspw. die Bekanntheit des Zertifikats ausgenutzt wird. Durch eine unabhängige Prüfung können einerseits die Qualität der internen Prozesse (bspw. der Administrationsprozesse) sowie die Effizienz verbessert werden. Andererseits können aber auch Hinweise zur Rechtssicherheit und IT-Sicherheit des Cloud-Dienstes gegeben werden. So könnten bspw. durch einen im Rahmen der Zertifizierung durchgeführten Penetrationstest Schwachstellen des Cloud-Dienstes identifiziert und anschließend behoben werden. Ferner können Cloud-Anbieter sich durch eine erhöhte Transparenz, welche mit einer Zertifizierung geschaffen werden kann, besser am Markt positionieren. Gerade kleine und mittlere Unternehmen (KMU) sehen in der Zertifizierung Chancen, Wettbewerbsvorteile gegenüber anderen Cloud-Anbietern erzielen zu können.

Auch für Cloud-Kunden bergen Zertifizierungen Vorteile.[11] So fehlen (potenziellen) Cloud-Kunden das Wissen oder die Kontrollmöglichkeiten, ob ein Cloud-Dienst rechtskonform ist oder sicher mit den eigenen Daten umgeht. Für einen unerfahrenen Cloud-Kunden geben Zertifikate eine erste Orientierung, denn sie machen auf Basis einer fachlich geeigneten und unabhängigen Prüfung Aussagen über die Qualität und Vertrauenswürdigkeit eines Cloud-Dienstes. Insbesondere im Hinblick auf das Niveau von Sicherheit und Datenschutz, welches durch einen Cloud-Dienst erfüllt wird, können Zertifizierungen Transparenz schaffen und Bedenken von Cloud-Kunden abbauen. Ein Zertifikat stellt auch ein Mittel zur Risikominimierung für Cloud-Kunden dar, da sie wiederrum ihren Kunden einen Nachweis zur Verfügung stellen können, dass sie einen sicheren Cloud-Dienst nutzen.

---

9 *Neubauer/Weiss/Lins/Sunyaev*, Vergleich existierender Zertifizierungen zum Nachweis vertrauenswürdiger Cloud-Services, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 81.

10 *Lins/Schneider/Sunyaev* (Fn. 2), 18 ff.

11 *Lins/Schneider/Sunyaev* (Fn. 2), 18 ff.

### *3. Datenschutzzertifizierungen*

Vor kurzem haben insbesondere Datenschutzzertifizierungen an großer Bedeutung gewonnen. Art. 42 und Art. 43 DSGVO regeln auf europäischer Ebene erstmalig die datenschutzrechtliche Zertifizierung als Nachweis dafür, dass die Datenschutz-Grundverordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.[12] Dadurch legt die Datenschutz-Grundverordnung die Grundsteine für die Entwicklung von technologiespezifischen datenschutzrechtlichen Zertifizierungsverfahren. Gerade bei hoch komplexen und in unterschiedlichen Dienst-Modellen vorkommenden Technologien wie dem Cloud Computing wird ein Unternehmen, das seine Datenverarbeitung im Rahmen einer Auftragsverarbeitung in die Cloud auslagern möchte, kaum eigenständig beurteilen können, ob ein Cloud-Anbieter die von Art. 28 Abs. 1 DSGVO geforderten „hinreichenden Garantien" dafür bietet, „dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen" der Grundverordnung erfolgt. Dies gilt insbesondere, da es Cloud-Kunden an Kontrollmöglichkeiten fehlt, um überprüfen zu können, ob ein Cloud-Dienst fortlaufend die an ihn gestellten rechtlichen Anforderungen erfüllt.[13] Da Art. 28 Abs. 5 DSGVO erklärt, dass die Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO durch einen Auftragsverarbeiter als Faktor für den Nachweis der in Art. 42 Abs. 1 und 4 DSGVO geforderten „hinreichenden Garantien" herangezogen werden kann,[14] ist es nicht verwunderlich, dass eine Vielzahl von neuen Zertifizierungsverfahren entwickelt werden. Auch das vom Bundesministerium für Wirtschaft und Energie geförderte Forschungsprojekt „*European Cloud Service Data Protection Certification (AUDITOR)*"[15] verfolgt das Ziel, eine nachhaltig anwendbare EU-weite Datenschutzzertifizierung von Cloud-Diensten zu konzeptionieren, exemplarisch umzusetzen und anschließend zu erproben.

---

12 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, Die Zertifizierung von Cloud-Diensten nach der DSGVO, DuD 2019, 225, 226.

13 *Lins/Schneider/Sunyaev*, Trust is good, control is better: creating secure clouds by continous auditing, IEEE Trans. Cloud Comput. 6 (2018), 890, 890 ff.

14 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, DuD 2019 (Fn. 12), 226.

15 *Roßnagel/Sunyaev/Meier/Batman/Lins/Teigeler*, AUDITOR: Neues Forschungsprojekt zur Datenschutz-Zertifizierung von Cloud-Diensten nach der DS-GVO, ZD-Aktuell 2017, 05900.

## III. Kontinuierliche Zertifizierungen von Cloud-Diensten

### 1. Probleme klassischer Zertifizierungen

Die klassische Zertifizierung von Cloud-Diensten und anderen Technologien stellt eine retrograde, statische und (überwiegend) von Menschen durchgeführte Methode der Bewertung von IT-Ressourcen dar.[16] Bei der Zertifizierung werden mehrere Ermittlungstätigkeiten durchgeführt, um vollständige Informationen über die Erfüllung der im Kriterienkatalog festgelegten Zertifizierungskriterien durch den Cloud-Dienst zu erhalten.[17] Hierzu zählen unter anderem Dokumentenprüfungen, die Durchführung von Interviews, Vor-Ort-Begutachtungen, Entwicklungsbegutachtungen oder technische Sicherheitstests. Zur Durchführung dieser Ermittlungstätigkeiten setzen Zertifizierungsstellen meist Auditoren (bspw. eigene oder externe Prüfer oder unabhängige Prüfstellen) ein. Im Anschluss entscheidet die Zertifizierungsstelle auf Grundlage des Prüfberichts und der Bewertung über die Erteilung des Zertifikats. Die vergebenen Cloud-Dienst-Zertifikate haben eine feste Gültigkeitsdauer von meist 1-3 Jahren.[18] Während der Gültigkeitsdauer werden öfters jährliche Überwachungsaudits durchgeführt.[19] Ein Überwachungsaudit umfasst systematische, sich wiederholende Ermittlungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Zertifizierung. Aufgrund von (stichprobenartigen) Zwischenprüfungen hat die Zertifizierungsstelle dabei festzustellen, ob ein zertifizierter Cloud-Dienst die Zertifizierungskriterien weiterhin erfüllt. Sollten bei der Überwachung Verstöße oder Abweichungen identifiziert werden, kann die Zertifizierungsstelle unter anderem das Zertifikat zeitweise aussetzen (bspw. bis zur Behebung durch den Cloud-Anbieter) oder vollständig widerrufen.

Die Durchführung von traditionellen Zertifizierungsprozessen erfordert eine gewisse Stabilität des Bewertungsgegenstandes, damit davon ausgegangen werden kann, dass die Prüfergebnisse über die gesamte Geltungszeitspanne identisch bleiben.[20] Da Cloud-Dienste sich durch dynamische

16 *Lins/Grochol/Schneider/Sunyaev*, Dynamic Certification of Cloud Services: Trust, but Verify!, IEEE Secur. Privacy 14 (2016), 66, 66 f.
17 *Lins/Schneider/Sunyaev* (Fn. 2), 94.
18 *Lins/Schneider/Sunyaev*, IEEE Trans. Cloud Comput. 6 (2018) (Fn. 13), 890 f.
19 *Lins/Schneider/Sunyaev* (Fn. 2), 94.
20 *Stephanov/Banse*, Ansatz der dynamischen Zertifizierung, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 114 ff.

Charakteristiken, eine schnelllebige Technologie und eine sich stetig verändernde Umwelt auszeichnen, ist jedoch die Einhaltung von Zertifizierungskriterien über die Geltungszeitspanne stark gefährdet.[21] Auch aus organisatorischer Sicht sind fortlaufende Veränderungen des Cloud-Dienstes erforderlich. So erfordern beispielweise neue Markteintritte, ein hoher Wettbewerbsdruck und die stetigen Veränderungen der Präferenzen von Cloud-Kunden, dass Cloud-Anbieter schnell auf sich abzeichnende Umweltveränderungen reagieren und ihre Cloud-Dienste, Strategien, Strukturen und das Tagesgeschäft entsprechend anpassen. Auch Änderungen in der IT-Umgebung, wie das Auftreten neuer Schwachstellen, erfordern von Cloud-Anbietern, ihre Prozesse anzupassen und ihre Mitarbeiter entsprechend zu schulen; andernfalls können schädliche Schwachstellen den Cloud-Dienst gefährden. Diese schnellen Änderungen der Geschäftsabläufe im laufenden Betrieb führen dazu, dass die anfänglichen Prozessspezifikationen, die im Rahmen einer Zertifizierung überprüft wurden, oft nicht mehr der Wirklichkeit entsprechen.

Bei einer bisherigen jährlichen (strichprobenartigen) Überwachung der Einhaltung von Zertifizierungskriterien können Abweichungen oder Verstöße teilweise erst lange nach deren Auftreten erkannt werden.[22] Da das ausgestellte Zertifikat dennoch weiterhin suggeriert, dass die Anforderungen erfüllt sind, kann ein Cloud-Kunde mögliche Verstöße nicht erkennen. Es wird daher insbesondere im Cloud-Kontext, aber auch in anderen schnelllebigen und dynamischen IT-Umgebungen, ein neuer Ansatz zur Durchführung von Zertifizierungen benötigt.

### 2. *Automatisierung von Zertifizierungsprozessen zur Schaffung von Vertrauen und Transparenz*

Um den beschriebenen Problemen entgegenzuwirken und fortlaufend die Einhaltung der Kriterien sicherzustellen, ist der Einsatz von kontinuierlichen Zertifizierungsprozessen möglich. Durch eine *kontinuierliche Zertifizierung* wird ein innovativer, (semi-)automatisierter Zertifizierungsprozess eingeführt, welcher die fortlaufende Überwachung von kritischen Parame-

---

21 *Lins/Schneider/Szefer/Ibraheem/Sunyaev*, Designing Monitoring Systems for Continuous Certification of Cloud Services, Communications of the Association for Information Security 44 (2019), 406, 406 ff.

22 *Lins/Sunyaev*, Konzeptionelle Architektur von dynamischen Zertifizierungen, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 121 ff.

tern eines Cloud-Dienstes ermöglicht.[23] Ein kontinuierlicher Zertifizierungsprozess umfasst automatisierte Überwachungs- und Auditierungstechniken, welche eine fortlaufende Ermittlung, Bewertung und Entscheidung ermöglichen, sowie Mechanismen zur transparenten Bereitstellung von zertifizierungsrelevanten Informationen, um die Einhaltung der Zertifizierungskriterien kontinuierlich zu bestätigen.[24] Das Konzept der kontinuierlichen Zertifizierung wurde maßgeblich im Forschungsprojekt „*Next Generation Certification*" (NGCert) erstellt und realweltlich erprobt,[25] welches vom Bundesministerium für Bildung und Forschung gefördert wurde.

Der kontinuierliche Zertifizierungsprozess kann abstrakt als sich wiederholender Zyklus verstanden werden. Dabei werden nacheinander und fortlaufend vier Teilprozesse durchgeführt: (1) semi- oder vollständig automatisierte Datenerhebung und -übermittlung; (2) semi- oder vollständig automatisierte Datenanalyse; (3) Zertifikatsausstellung; und (4) Prozessanpassung.[26] Eine kontinuierliche Zertifizierung erfordert von einer Zertifizierungsstelle, regelmäßig umfangreiche Datensätze zu erheben und zu bewerten.[27] Zur Erhebung von Daten können *test-basierte Verfahren* oder *monitoring-basierte Verfahren* eingesetzt werden. So werden bspw. bei monitoring-basierten Verfahren die Daten vom Cloud-Anbieter selbst erhoben und für die Zertifizierungsstelle zugänglich gemacht. Die Zertifizierungsstelle führt anschließend eine fortlaufende Analyse der zusammengetragenen und übermittelten Daten durch und prüft, ob die Zertifizierungskriterien weiterhin erfüllt sind. Zur Bewertung der Daten können bspw. Entscheidungsunterstützungssysteme eingesetzt werden, welche es einer Zertifizierungsstelle erlauben, die zertifizierten Cloud-Dienste automatisch zu bewerten, Abweichungen zu entdecken und bei Nichteinhaltung von Anforderungen einen Alarm auszulösen oder weitere Maßnahmen zu ergreifen (bspw. Aussetzung des Zertifikats).[28] Nach der Datenanalyse veranlasst eine Zertifizierungsstelle die Aktualisierung der Gültigkeit des Zertifikats und informiert gegebenenfalls die Öffentlichkeit und Cloud-Kunden zu wichtigen Themenbereichen, wie bspw. festgestellte Abweichungen oder

23 *Lins/Schneider/Sunyaev*, IEEE Trans. Cloud Comput. 6 (2018) (Fn. 13), 890 f.
24 *Lins/Grochol/Schneider/Sunyaev*, IEEE Secur. Privacy 14 (2016) (Fn. 16), 67 f.
25 *Banse/Stephanow*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.) (Fn. 3), 1 ff.
26 *Lins/Grochol/Schneider/Sunyaev*, IEEE Secur. Privacy 14 (2016) (Fn. 16), 67 f.
27 *Lins/Schneider/Sunyaev*, IEEE Trans. Cloud Comput. 6 (2018) (Fn. 13).
28 *Hunton/Rose*, 21st Century Auditing: Advancing Decision Support Systems to Achieve Continuous Auditing, Accounting Horizons 24 (2010), 297, 297 ff.

kritische Defizite.[29] Schließlich muss ein kontinuierlicher Zertifizierungsprozess fortlaufend angepasst werden, um die Herausforderungen und Dynamiken eines sich ständig verändernden Umfelds und einer unsicheren Umgebung zu bewältigen.

Im Gegensatz zu jährlichen Überwachungsaudits ermöglicht eine Automatisierung von Prüfprozessen, zeitnah kritische Defekte bereits bei Auftreten zu ermitteln und zu untersuchen, und dadurch die Glaubwürdigkeit der Zertifizierungen und die Vertrauenswürdigkeit in den Cloud-Dienst zu erhöhen.[30] Fortlaufende (automatisierte) Überprüfungen ermöglichen es zudem, Veränderungen eines Cloud-Dienstes während dessen produktiven Betriebs zu detektieren und die Auswirkungen dieser Veränderungen auf die Erfüllung der Kriterien eines Zertifikates zu bewerten. Im Gegensatz zur herkömmlichen Zertifizierung berücksichtigt eine kontinuierliche Zertifizierung bei der Beurteilung der Einhaltung der Zertifizierung den tatsächlichen Status quo der Cloud-Infrastruktur und informiert die Cloud-Kunden letztlich durch eine transparente und aktuelle Zertifizierungsdarstellung sowohl über Verbesserungen der Infrastruktur (bspw. bessere Dienstqualität) als auch über Ausfälle (bspw. Datenverluste).

## *IV. Kontinuierliche Zertifizierung am Beispiel von Datenschutzzertifizierungen*

Ziel einer kontinuierlichen Zertifizierung ist die fortlaufende Überprüfung der Einhaltung von Zertifizierungskriterien durch einen Cloud-Dienst. Hierbei muss jedoch der genaue Umfang der Prüfprozesse festgelegt werden, da nicht jedes Zertifizierungskriterium automatisiert prüfbar ist bzw. eine automatisierte Überprüfung fordert. Im Folgenden werden die Kriterien des *AUDITOR-Kriterienkatalogs*[31] exemplarisch untersucht und diskutiert, ob eine fortlaufende Überprüfung erforderlich ist, um sicherzustellen, dass die Kriterien auch tatsächlich eingehalten werden. Zudem wird eine Einschätzung hinsichtlich der Automatisierbarkeit für entsprechende Prüfungen gegeben.

Die Analyse des AUDITOR-Kriterienkatalogs zeigt, dass eine Vielzahl von Zertifizierungskriterien fortlaufend überprüft werden sollte. Die Kern-

29 *Lins/Grochol/Schneider/Sunyaev*, IEEE Secur. Privacy 14 (2016) (Fn. 16), 68.

30 *Lins/Schneider/Szefer/Ibraheem/Ali*, Communications of the Association for Information Security 44 (2019) (Fn. 21), 410 ff.

31 *Roßnagel/Sunyaev/Lins/Maier/Teigeler*, AUDITOR-Kriterienkatalog: Entwurfsfassung 0.9, 2019.

punkte des Kriterienkatalogs bilden die normativen Kriterien, die aus den einschlägigen Normen der Datenschutz-Grundverordnung zur Auftragsverarbeitung entwickelt worden sind.[32] Darüber hinaus werden zu jedem Kriterium rechtliche Erläuterungen und Hinweise, wie der Cloud-Anbieter die Kriterien umsetzen und ihre Erfüllung im Zertifizierungsverfahren nachweisen kann, gegeben. Thematisch zusammenhängende Kriterien werden in sieben einzelne Kapitel gegliedert. Das Kapitel VII des Kriterienkatalogs enthält die Kriterien an den Cloud-Anbieter als Verantwortlichen für die Datenverarbeitung, die zur Durchführung des Auftrags mit dem Cloud-Kunden für die Erbringung, Nutzung und Abrechnung des Cloud-Dienstes erforderlich sind. Aufgrund der hohen Überschneidungen zu den vorherigen Kapiteln des Kriterienkatalogs wird Kapitel VII nicht weiter betrachtet.

### *1. Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung*

Kapitel I enthält Kriterien, die eine rechtsverbindliche Vereinbarung des Cloud-Anbieters mit dem Cloud-Kunden über die Auftragsverarbeitung betreffen.[33] Die Kriterien bilden die einzelnen gesetzlichen Anforderungen von Art. 28 Abs. 3 DSGVO ab, bspw. hinsichtlich der Bestimmung von Gegenstand und Dauer der Verarbeitung, der Festlegung der Weisungsbefugnisse des Cloud-Kunden gegenüber dem Cloud-Anbieter oder der Verantwortung des Cloud-Anbieters, die mit der Datenverarbeitung betrauten Mitarbeiter zur Vertraulichkeit zu verpflichten. Im Rahmen der Zertifizierung kann der Cloud-Anbieter den Nachweis erbringen, indem er unter anderem Dokumentationen zur rechtsverbindlichen Vereinbarung mit diesen Angaben vorlegt (beispielweise Vertragsmuster, -vorlagen oder -instanzen).[34]

Die Einhaltung der Kriterien zur rechtsverbindlichen Vereinbarung sollte fortlaufend überprüft werden, um sicherzustellen, dass auch bei neuen Cloud-Kunden eine rechtskonforme Vereinbarung geschlossen wird. Zudem können interne Veränderungen dazu führen, dass Bestandteile der Vereinbarungen fortlaufend aktualisiert werden müssen (bspw. Anpassung der Angaben zu den technischen und organisatorischen Maßnahmen (TOM)). Zur automatisierten Überprüfung können Konzepte und Verfah-

32 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, DuD 2019 (Fn. 12), 227 f.
33 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, DuD 2019 (Fn. 12), 227.
34 *Roßnagel/Sunyaev/Lins/Maier/Teigeler* (Fn. 31), 15 ff.

ren eingesetzt werden, welche bereits zur Prüfung der Einhaltung von Service-Level-Agreements (SLA) angewendet werden. Um die Einhaltung von Vereinbarungen zu bewerten und zu validieren, müssen die Anforderungen an die Vereinbarungen und die Vereinbarungen selbst in eine formale, maschinen-verständliche Darstellung umgewandelt werden. Hierzu können unter anderem ontologiebasierte Darstellungen,[35] domänenspezifische Sprachen,[36] oder eine Kombination aus JSON, Formeln und Logiken verwendet werden.[37] Nach der formalen Spezifikation können automatisierte Überwachungsdienste in die Cloud-Infrastruktur eingebettet werden, welche notwendige Informationen zur Beurteilung der Einhaltung von Anforderungen (dynamisch) erheben.[38] Daher scheint insbesondere der Einsatz von monitoring-basierten Zertifizierungsverfahren für die Überwachung der Kriterien zur rechtsverbindlichen Vereinbarung möglich.

### *2. Rechte und Pflichten des Cloud-Anbieters*

Hoher Stellenwert kommt auch den zahlreichen Kriterien des Kapitels II zu den Rechten und Pflichten des Cloud-Anbieters zu.[39] So sind bspw. Kriterien formuliert worden, um die rechtlichen Anforderungen zur Datensicherheit aus Art. 32 DSGVO cloud-spezifisch zu konkretisieren. Ein Cloud-Anbieter soll kontinuierlich angemessene Sicherheitsmaßnamen gegen interne und externe Angriffe nachweisen können, um einen unbefugten Zugriff zu verhindern. Hierzu zählen bspw. sämtliche Standardmaßnahmen für den Schutz des Cloud-Hosts, d. h. Host Firewalls, Network-Intrusion-Detection-Systeme, Applikationsschutz, Antivirus und regelmäßige Integritätsüberprüfungen wichtiger Systemdateien.

Die fortlaufende Überprüfung der Cloud-Architektur weist ein hohes Automatisierungspotenzial unter der Verwendung von monitoring- und

---

35 *Lamparter/Luckner/Mutschler*, Formal Specification of Web Service Contracts for Automated Contracting and Monitoring, in: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007, 63.

36 *Emeakaroha/Netto/Calheiros/Brandic/Buyya/De Rose*, Towards autonomic detection of SLA violations in cloud infrastructures, Future Generation Computer Systems 28 (2012), 1017.

37 *Goel/Kumar/Shyamasundar*, SLA Monitor: A System for Dynamic Monitoring of Adaptive Web Services, in: Proceedings of the Ninth IEEE European Conference on Web Services (ECOWS), 2011, 109.

38 *Lins/Schneider/Sunyaev* (Fn. 2), 152 f.

39 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, DuD 2019 (Fn. 12), 227 f.

test-basierten Verfahren auf.[40] Cloud-Anbieter überwachen bereits wesentliche Performanzparameter (bspw. Antwortzeitverhalten von Ressourcen) und ihre Cloud-Netzwerke (bspw. virtuelle Umgebungen und den Datenaustausch zwischen Rechenzentren) und führen Kapazitäts- und Stresstests zur Feststellung der Kapazitätsgrenzen durch. Durch die Verwendung von automatisierten Penetrationstests und Werkzeugen zur Durchführung von Schwachstellenanalysen können auch erste Indikatoren über die Robustheit der Architektur und der Mandantentrennung ermittelt werden. Netzwerk-Management-Tools ermöglichen zudem die Detektion von unautorisierter Hardware und Software innerhalb eines Netzwerkes, und können daher bei der Beurteilung sicherheitsrelevanter Kriterien herangezogen werden. Insbesondere die Prozesse zur Durchführung eines Schwachstellen- sowie Event- und Incident-Managements wurden in der Vergangenheit durch die Verwendung von Software-Werkzeugen zunehmend automatisiert. Moderne Schwachstellen-Scanner finden Softwarefehler proaktiv und liefern einen schnellen und einfach Weg, Sicherheitsrisiken zu messen, veraltete Softwareversionen zu identifizieren, Sicherheitsrichtlinien des Unternehmens zu überprüfen und Berichte und Warnungen zu identifizierten Schwachstellen zu generieren. Eine automatisierte Erkennung von Schwachstellen und Softwarefehlern ermöglicht somit einen Rückschluss auf die Erfüllung von sicherheitsrelevanten Zertifizierungskriterien. Weitere Überprüfungen von Kriterien weisen ebenfalls ein hohes Automatisierungspotenzial auf, darunter der Einsatz von automatisierten Tests zur Feststellung der Stärke der Transportverschlüsselung sowie die Überwachung der Verfügbarkeit und Wiederherstellbarkeit von Backups, um die Wiederherstellbarkeit nach physischem oder technischem Zwischenfall fortlaufend sicherstellen zu können.

Viele Kriterien im Kapitel II können zumindest indirekt über die automatisierte Analyse von Protokollen kontinuierlich überprüft werden. Dazu zählen beispielsweise die fortlaufende Aktualisierung des Datensicherheitskonzepts, die Protokollierung von Eingaben, Veränderungen und Löschungen personenbezogener Daten oder Protokolle zur Unterstützung der Cloud-Kunden bei der Wahrung der Betroffenenrechte. So wurden Techniken zur Überprüfung der Einhaltung von Datenschutzbestimmungen anhand von Protokollen entwickelt.[41] Dazu werden maschinenlesbare

40 *Lins/Schneider/Sunyaev* (Fn. 2), 113 f.

41 *Accorsi*, Automated Privacy Audits to Complement the Notion of Control for Identity Management, in: Leeuw/Fischer-Hübner/Tseng/Borking (Hrsg.), Policies and Research in Identity Management, New York 2008, 39.

Richtlinien festgelegt und das Protokoll in eine Baumstruktur umgewandelt. Durch das sukzessive Entfernen von Baumknoten, wenn diese mit den Richtlinien übereinstimmen, entsteht ein Baum, der gefundene Richtlinienverletzungen enthält. Ähnlich kann durch heuristische Protokollinspektionstechniken überprüft werden, ob verschiedene Anwendungen tatsächlich auf einer Cloud-Infrastruktur ausgeführt werden, darunter Malware-Schutz, Antivirensoftware oder verbotene Anwendungen.[42] Bei der Auswertung von Protokollen können auch Data-Mining-Techniken eingesetzt werden, um bspw. Systemanomalien zu erkennen.[43]

Allerdings erscheint die automatisierte Überprüfung einiger Kriterien zum jetzigen Stand der Forschung schwierig. So ist die Feststellung, ob Anforderungen zur Pseudonymisierung und Anonymisierung eingehalten werden, nur begrenzt automatisch möglich. Gleichermaßen ist die kontinuierliche Überwachung des Sicherheitsbereichs und der Zutrittskontrolle durch physische Maßnahmen, wenn überhaupt, so nur auf unwirtschaftliche Art und Weise kontinuierlich zu prüfen.

### *3. Datenschutz-Managementsystem des Cloud-Anbieters*

Kapitel III des Kriterienkatalogs behandelt das Datenschutzmanagementsystem des Cloud-Anbieters.[44] Das Kapitel enthält bspw. Kriterien für die Benennung eines Datenschutzbeauftragten (DSB) nach Art. 37-39 DSGVO und § 38 BDSG, für die Meldung von Datenschutzverletzungen nach Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f DSGVO und für die Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 2 DSGVO.

Eine kontinuierliche Zertifizierung erscheint nicht für jedes Kriterium notwendig, darunter die Benennung des DSB oder das Führen eines Verarbeitungsverzeichnisses. Auch ist eine kontinuierliche Überprüfung nur begrenzt möglich, da es sich insbesondere um organisatorische Prozesse handelt, die zu prüfen sind. So können Auditoren Informationen aus Workflow-Management-Systemen auslesen, um die korrekte Bearbeitung von Prozessen nachvollziehen zu können.[45] Auch können über die Durchfüh-

---

42 *Jiang/Hassan/Hamann/Flora*, An automated approach for abstracting execution logs to execution events, J. Softw. Maint. Evol. Res. Pract. 20 (2008), 249.

43 *Fu/Lou/Wang/Li*, Execution Anomaly Detection in Distributed Systems through Unstructured Log Analysis, in: Proceedings. The Ninth IEEE International Conference on Data Mining, 2009, 149.

44 *Maier/Lins/Teigeler/Roßnagel/Sunyaev*, DuD 2019 (Fn. 12), 228.

45 *Lins/Schneider/Sunyaev* (Fn. 2), 116 f.

rung von Prozessen durch die Verwendung von modernen Protokollgenerierungs- und Analyseverfahren wie Process Mining Daten erzeugt werden.[46] So lässt sich durch Protokollanalysen die Meldung von Datenschutzverletzungen feststellen. Allerdings ist die Auswertung von erhobenen Daten aufgrund komplexer Prozessstrukturen und schwer formalisierbaren Prozessspezifikationen meist nur manuell möglich.

### *4. Datenschutz durch Systemgestaltung*

Das Kapitel IV des Kriterienkatalogs verpflichtet den Cloud-Anbieter zu Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen.[47] Die Maßnahmen, um diese Kriterien umzusetzen, sind sehr vielfältig. Sie reichen von der Implementierung eines datensparsamen Logins für den Zugang zum Cloud-Dienst, über Rollen- und Berechtigungskonzepte für die Administration der verarbeiteten Daten bis hin zu Löschkonzepten für die Löschung dieser Daten. Diese Vielfalt führt dazu, dass Auditoren eine Vielzahl an Ermittlungen durchführen, darunter bspw. einen Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen, eine testweise Dienstnutzung (bspw. Überprüfung der Funktionen und Maßnahmen gemäß Dienstbeschreibung) oder eine stichprobenartige Quellcodeanalyse. Da sich die Systeme und die Voreinstellungen durch fortlaufende interne Veränderungen (bspw. Hinzufügen neuer Funktionen oder Änderungen am Quellcode) stetig verändern, ist die kontinuierliche Prüfung des Datenschutzes durch Systemgestaltung sinnvoll.

Es bietet sich an, die kontinuierliche Zertifizierung in die Change-Management-Prozesse des Cloud-Anbieters zu integrieren, um dadurch anlassbezogene Prüfungen zu initiieren. So kann bspw. ein Cloud-Anbieter die Zertifizierungsstelle über wesentliche Änderungen am Cloud-Dienst informieren, sodass diese je nach Umfang oder Kritikalität der Änderungen gezielte automatisierte Tests durchführen kann. Im Rahmen der Softwareentwicklung kommen zum Beispiel bereits eine Vielzahl von automatisierten Werkzeugen und Methoden zum Testen von Funktionalität, zur Erzeugung von Fehlerzuständen oder zur Überprüfung der Systemreakti-

---

46 *van der Aalst/Medeiros*, Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance, Electronic Notes in Theoretical Computer Science 121 (2005), 3.

47 *Roßnagel/Sunyaev/Lins/Maier/Teigeler* (Fn. 31), 46 f.

on zum Einsatz.[48] Auch die Untersuchung von Quellcode durch automatisierte Tests ist möglich.[49] Zur Auditierung können ebenfalls automatisierte Werkzeuge zum Testen von graphischen Oberflächen eingesetzt werden, die maschinelles Sehen unterstützen und damit die Interaktion mit einem Cloud-Dienst simulieren können, um unter anderem auf datenschutzfreundliche Voreinstellungen zu prüfen.[50]

Grundsätzlich ist es auch möglich, Systemdesigns automatisiert zu analysieren, um Sicherheitsschwachstellen oder Compliance-Probleme zu identifizieren.[51] Process-Mining-Techniken und teilautomatisierte Modellbewertungsalgorithmen können zur Unterstützung dieser Aufgaben eingesetzt werden. Allerdings gestaltet sich ein Vergleich von Designspezifikationen mit der tatsächlichen Ausgestaltung des Cloud-Dienstes in der Praxis aufgrund des schnelllebigen Cloud-Umfelds als schwierig. Initial definierte Spezifikationen können schnell veraltet sein, wodurch ein Vergleich nicht mehr möglich ist.

### *5. Subauftragsverarbeitung*

Kapitel V definiert Kriterien zur Gewährleistung eines gleichbleibenden Datenschutzniveaus trotz des Einsatzes weiterer Auftragsverarbeiter im Rahmen von Subauftragsverarbeitungen.[52] Dazu zählt auch, dass der Cloud-Anbieter sicherstellt, dass ein Cloud-Dienst unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der Cloud-Kunde vorher in diese Subauftragsverarbeitung in Schrift- oder Textform eingewilligt hat. Auch muss der Cloud-Anbieter den Cloud-Kunden über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter informieren. Die Zertifizierungsstelle sollte im Sinne der Transparenz überprüfen, ob der Cloud-Anbieter auch tatsächlich seine Cloud-Kunden hinreichend über neue Subauftragsverarbeiter informiert. Da die Einschaltung von weiteren Subauftragsverarbeitern für einen Cloud-Anbieter meist ein aufwendiger und manueller Prozess ist (beispielweise Einsichtnahme, ob Subauftragsverarbeiter geeignete Garantien zur Einhaltung der Daten-

48 *Lins/Schneider/Sunyaev* (Fn. 2), 113.
49 *Chess/McGraw*, Static analysis for security, IEEE Secur. Privacy 2 (2004), 76.
50 *Chang/Yeh/Miller*, GUI testing using computer vision, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10), 2010, 1535.
51 *Lins/Schneider/Sunyaev* (Fn. 2), 115 ff.
52 *Roßnagel/Sunyaev/Lins/Maier/Teigeler* (Fn. 31), 48 ff.

schutz-Grundverordnung vorweisen kann), scheint jedoch eine kontinuierliche Überprüfung nicht erforderlich. Veränderungen an der Wertschöpfungskette werden in der Regel seltener geschehen, sodass eine Überprüfung im Rahmen der jährlichen Überwachungsaudits ausreichend erscheint.

### 6. *Datenverarbeitung außerhalb der EU und des EWR*

Die Datenverarbeitung außerhalb der EU und des EWR regelt Kapitel VI. So fordern die Kriterien bspw. den Nachweis geeigneter Garantien für die Datenübermittlung und die Benennung eines Vertreters, wenn die Auftragsverarbeitung außerhalb der EU und des EWRs stattfinden soll.[53] Die kontinuierliche Gewährleistung von geeigneten Garantien für die Datenübermittlung und die korrekte Vertreterbenennung können einerseits nur schwer automatisiert überprüft werden. Andererseits ist eine fortlaufende Überprüfung nicht erforderlich, da hierbei keine Veränderungen zwischen den einzelnen Überwachungsaudits zu erwarten sind.

Allerdings kann durch Anwendung von innovativen, test-basierten Verfahren der tatsächliche Ort der Datenverarbeitung fortlaufend überwacht werden.[54] So wurde im Rahmen des Forschungsprojektes *NGCert* ein Klassifikationsverfahren basierend auf Maschine-Learning entwickelt, welches einen Standort anhand von der Zeit, die ein Datenpaket braucht, um den Standort zu erreichen, klassifiziert. In einem Test wurde nachgewiesen, dass dieses Klassifikationsverfahren durchschnittlich 92,97 % der Orte korrekt klassifiziert, sodass bereits ein hoher Reifegrad erreicht werden konnte, jedoch eine fehlerfreie Feststellung zum aktuellen Stand der Technik noch nicht möglich ist. Die kontinuierliche Überwachung der Datenlokation ist gerade im Cloud-Umfeld von besonderer Bedeutung, denn die Migration von virtuellen Cloud-Ressourcen von einem geographischen Ort zu einem anderen, d.h. von einem Rechenzentrum in ein anderes, ist eine Standardfunktion zum Ausgleich von Lastspitzen zwischen Rechenzentren eines Anbieters.

---

53 *Roßnagel/Sunyaev/Lins/Maier/Teigeler* (Fn. 31), 51 f.

54 *Stephanow/Banse*, Beispielhaftes Testszenario: Geolokation, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 240 ff.

## V. Fazit und Ausblick

Eine Zertifizierung von Cloud-Diensten zielt darauf ab, Vertrauen zu etablieren und die Akzeptanz von Cloud-Computing zu erhöhen. Sowohl kleine, mittlere und große Cloud-Anbieter als auch Cloud-Kunden können von Cloud-Zertifizierungen gleichermaßen profitieren. So können bspw. kleinere und regionale Cloud-Anbieter durch praxisorientierte und marktrelevante Zertifizierungen für ihre Cloud-Dienste am Markt hervorstechen und einen größeren Kundenstamm gewinnen. Cloud-Kunden dienen Zertifizierungen und deren Kriterienkataloge wiederrum als Entscheidungshilfe, um Cloud-Angebote zu bewerten, zu vergleichen und auszuwählen.

Ungeachtet der vielen Herausforderungen bei der Einführung einer kontinuierlichen Zertifizierung birgt diese große Vorteile, darunter Transparenz über einen Cloud-Dienst, Erhöhung der Glaubwürdigkeit der Zertifizierungen und eine fortlaufende Überprüfung durch einen unabhängigen Dritten. Auch in Themenfeldern wie dem Datenschutz scheint eine kontinuierliche Zertifizierung zu großen Teilen sinnvoll und technisch machbar. Während marktführende Cloud-Anbieter und Zertifizierungs- und Prüfstellen das notwendige Knowhow, die personellen und finanziellen Ressourcen haben, um eine Automatisierung von Prüfprozessen mit ausgewählten Partnern umzusetzen, mangelt es jedoch gerade KMU an den notwendigen Ressourcen und dem Fachwissen hierfür. Dadurch stehen KMU vor großen Herausforderungen bei der Umsetzung der kontinuierlichen Zertifizierung, obwohl diese von einer Automatisierung der Prüfprozesse am meisten profitieren könnten. Es sind daher innovative Lösungsansätze für KMU von Nöten, um das gesamte Potenzial einer kontinuierlichen Zertifizierung ausschöpfen zu können.

Zur Lösung dieses Problems bietet sich insbesondere ein plattformbasierter Ansatz an. Durch die Entwicklung einer Plattform kann ein Ökosystem geschaffen werden, in dem sich unterschiedliche Interessengruppen vernetzten und verschiedene Dienste anbieten und nutzen können, die mit der kontinuierlichen Zertifizierung der Cloud-Sicherheit im Zusammenhang stehen. So können Synergien genutzt und vertrauenswürdige Angebote für die gesamte Wertschöpfungskette entwickelt werden. Cloud-Anbieter können sich mit der Plattform vernetzen, um fortlaufend Informationen über ihre angebotenen Dienste bereitzustellen. Prüfer und Software-Entwickler verschiedenster Domänen können als Anbieter für kontinuierliche Messverfahren in der Plattform auftreten, entweder die zur Verfügung gestellten Informationen nutzen oder eigene Datenerhebungen beim Cloud-Anbieter durchführen, und so Mehrwertdienste anbieten. Die erhobenen und analysierten Informationen über einen Cloud-Dienst kön-

nen wiederrum von Drittparteien wie Zertifizierungs- und Prüfstellen genutzt werden, um die Konformität mit geltenden (rechtlichen) Anforderungen (bspw. der Datenschutz-Grundverordnung) zu überprüfen. Auch können Datenschutzaufsichtsbehörden (zusätzliche) Informationen über die Einhaltung des Datenschutzes über eine derartige Plattform gewinnen. Um eine solche Plattform im Kontext einer kontinuierlichen Zertifizierung zu realisieren, besteht weiterer Forschungsbedarf, um ein Ökosystem zur Vernetzung aller Akteure zu schaffen und automatisierte und kontinuierliche Prüf- und Zertifizierungsmechanismen speziell auf die Bedürfnisse von KMU auszurichten.