Douglas Cunningham, Petra Hofstedt, Klaus Meer, Ingo Schmitt (Hrsg.): INFORMATIK 2015
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015

Dynamische Zertifizierung von Cloud Computing-Diensten: Eine rechtswissenschaftliche Betrachtung am Beispiel „Verfügbarkeit“

Ass. jur. Johanna M. Hofmann LL.M.[1]

Abstract: Dieser Beitrag betrachtet die dynamische Zertifizierung von Cloud-Diensten am Beispiel des Kriteriums „Verfügbarkeit“ aus rechtswissenschaftlicher Sicht.[2] Nach der Einführung in die Problematik der Zertifizierung von Cloud Computing-Diensten (2) und der Vorstellung der Grundzüge der dynamischen Zertifizierung (3) wird das methodische Vorgehen zur rechtlichen Überprüfung von automatisiert und kontinuierlich zu prüfenden Anforderungen dargestellt (4). Diese Methodik wird sodann auf das Beispiel „Verfügbarkeit“ angewendet (5).

Keywords: Dynamische Zertifizierung; Cloud Computing; Kontrollpflicht des Auftraggebers; Methode KORA; Verfügbarkeit;

1 Einleitung

Mit Cloud Computing bezeichnet man die Auslagerung der eigenen Datenverarbeitung in eine vernetzte Rechnerarchitektur, das heißt „in die Wolke“.[3] Datenschutzrechtlich handelt es sich beim Cloud Computing in aller Regel um eine sogenannte Auftragsdatenverarbeitung.[4] Vielfach sind die „in die Cloud“ übertragenen Daten personenbezogen.[5] Die Übertragung ist dann nach dem Bundesdatenschutzgesetz zu beurteilen.[6] Die Auftragsdatenverarbeitung ist ein Sonderfall der Verantwortungszuweisung. Bei Vorliegen der Voraussetzungen[7] liegt keine Übermittlung personenbezogener Daten vor. Für die Zulässigkeit der Datenverarbeitung durch den Cloud-Dienst-Anbieter[8] ist entgegen des Grundsatzes aus § 4 Abs. 1 BDSG keine gesetzliche oder rechtsgeschäftliche Ermächtigung oder gesetzliche Gebotsnorm

[1] Wissenschaftliche Mitarbeiterin in der Projektgruppe für verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel, Pfannkuchstr. 1, 34109 Kassel, j.hofmann@uni-kassel.de.

[2] Gegenstand dieses Beitrags sind Ergebnisse des Forschungsprojekts „Next Generation Certification“ (NGCert), das vom Bundesministerium für Bildung und Forschung als Teil des Themenfeldes “Forschung für Sicheres Cloud Computing” im Rahmen der Hightech-Strategie der Bundesregierung gefördert wird (ngcert.de).

[3] *Weichert*, DuD 2010, 679. Zur gängigen Definition, den drei Dienstmodellen (Software as a Service, Infrastructure as a Service und Plattform as a Service) und den vier Erscheinungsformen (Private-/Public-/Hybrid- und Community Cloud) *Mell/Grance* (National Institute of Standards and Technologie (NIST), The NIST Definition of Cloud Computing, September 2011, 2 ff..

[4] § 11 Bundesdatenschutzgesetz (BDSG).

[5] Vgl. § 3 Abs. 1 BDSG.

[6] *Roßnagel*, Handbuch Datenschutzrecht, 2003, Kap. 7.9, Rn. 59.

[7] §§ 3 Abs. 8 Satz 3, 11 BDSG.

[8] „Cloud-Anbieter“.

erforderlich. Übertragen auf das Cloud Computing bedeutet dies, dass der Cloud-Dienst-Kunde[9] (Auftraggeber) gemäß § 11 Abs. 1 Satz 1 BDSG die datenschutzrechtliche Verantwortlichkeit über diejenigen personenbezogenen Daten behält, die er oder die Anwender „in die Cloud" übertragen. Er bleibt für diese Daten derjenige, der über Zweck und Mittel der Datenverarbeitung entscheidet.[10] Der Cloud-Anbieter (Auftragnehmer) hingegen ist in diesem Verhältnis grundsätzlich keine verantwortliche Stelle, sondern hat die Daten entsprechend dem Vertrag über die Auftragsdatenverarbeitung sowie den Weisungen des Cloud-Kunden zu verarbeiten. Davon zu unterscheiden sind solche Daten, die nicht „in die Cloud" übertragen werden, sondern durch die Nutzung des Dienstes entstehen (z.B. Nutzungsdaten). Bei diesen kann es sich ebenfalls um personenbezogene Daten handeln.[11] Für deren Verarbeitung wird in der Regel der Cloud-Anbieter verantwortliche Stelle sein.[12]

Der Auftraggeber ist gemäß § 11 Abs. 2 Satz 1 BDSG verpflichtet, den Auftragnehmer „sorgfältig auszuwählen". Der Cloud-Kunde hat dabei zu überprüfen, ob der Cloud-Anbieter ein angemessenes Datenschutzniveau bietet.[13] Darüber hinaus hat sich der Auftraggeber „vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen".[14] Folglich ist der Cloud-Kunde verpflichtet, vor Beginn der Auftragsdatenverarbeitung und sodann in regelmäßigen Abständen die Einhaltung der Anforderungen und seiner Weisungen seitens des Cloud-Anbieters zu kontrollieren. Wie diese Kontrolle zu erfolgen hat, ist im Gesetz nicht ausdrücklich geregelt. Die Kontrollmöglichkeiten reichen von der persönlichen Vor-Ort-Kontrolle des Cloud-Kunden, über Selbstauditierungen des Cloud-Anbieters bis hin zu Bewertungen durch Dritte. Die persönliche Vor-Ort-Kontrolle ist dabei für beide Seiten mit Nachteilen verbunden. Der Cloud-Anbieter ist dazu verpflichtet, jedem einzelnen seiner Kunden die Ausübung der gesetzlichen Kontrollpflicht zu ermöglichen und hat gegebenenfalls Zutritt zu seinen Serverräumen zu gewähren. Dies kann einen erheblichen Zeit- und Geldaufwand bedeuten. Wesentlich schwerer wiegen allerdings die damit verbundenen Sicherheitsrisiken, die der Zutritt Betriebsfremder zu seinen Betriebsräumlichkeiten mit sich bringen kann. Hinsichtlich des Cloud-Kunden stößt eine Vor-Ort-Kontrolle auf die folgenden Schwierigkeiten: Zum einen kennt er den Speicherort der Daten regelmäßig

[9] Derjenige, der in vertraglicher Beziehung zum Cloud-Anbieter steht und die Cloud-Dienste bezieht („Cloud-Kunde"). Der Cloud-Kunde kann seinerseits Kunden haben, die hier der Klarheit halber als „Anwender" bezeichnet werden. Der Cloud-Anbieter ist derjenige, der die Cloud-Dienste entweder selbst oder durch die Hinzuziehung dritter Subunternehmer erbringt. Mit anderen Worten stellt der Cloud-Anbieter Software, Infrastruktur oder die Plattform zur Verfügung.

[10] *Dammann,* in: Simitis, BDSG 8. Aufl. 2014, § 3 BDSG Rn. 224. Ausführlich zur Definition der „verantwortlichen Stelle" die Artikel 29-Arbeitsgruppe Stellungnahme 05/2012 zum Cloud Computing („WP 196"), Kap. 3, 10 ff.

[11] *Boos/Kroschwald/Wicker*, ZD 2013, 207.

[12] Hierzu Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Stand 09.10.2014 („Düsseldorfer Kreis, Orientierungshilfe"), 9.

[13] *Petri,* in: Simitis, BDSG 8. Auflage 2014, § 11 BDSG Rn. 55.

[14] § 11 Abs. 2 Satz 4 BDSG.

nicht; zum anderen liegt der Speicherort möglicherweise in großer geographischer Entfernung zu seinem eigenen Standort. Es ist zudem denkbar, dass die jeweiligen Daten auf verschiedene Serverstandorte verteilt sind, es daher mit der Kontrolle eines einzigen Rechenzentrums zur Erfüllung der gesetzlichen Kontrollpflicht nicht getan wäre.

Die Unterstützung der Kontrollpflicht durch Dritte, stellt sich demgegenüber als besonders vorteilhaft dar. Auch ist die Aussage eines Dritten objektiver und daher glaubhafter als eine interessengeleitete Selbsteinstschätzung des Cloud-Anbieters.[15]

Konformitätsbewertungen im Bereich der Informationstechnologien (IT) werden in der Rechtswissenschaft uneinheitlich als Gütesiegel, Testate oder Zertifikate bezeichnet. Eine klare Abgrenzung ist in Ermangelung einer einheitlichen gesetzlichen Regelung noch nicht erfolgt. Auch unterscheiden sich tatbestandliche Voraussetzungen, Verfahren und Rechtsfolgen. Dieser Beitrag wird die Begriffe synonym für Bestätigungen über das Erfüllt-Sein von festgelegten Kriterien verwenden, die im Rahmen eines geregelten Konformitätsbewertungsverfahren durch eine akkreditierte Stelle vergeben werden.

2 Die Zertifizierung von Cloud Computing-Diensten

Bereits in den Gesetzesmaterialien,[16] aber auch unter den Aufsichtsbehörden[17] und in der Literatur[18] ist anerkannt, dass im Einzelfall alternative Gestaltungsformen zur persönlichen Vor-Ort-Kontrolle des Cloud-Kunden zulässig sein können. Die Heranziehung fachkundiger Aussagen Dritter, in Form von Zertifizierungen, ist eine dieser Möglichkeiten. Diese Möglichkeit scheint besonders vorteilhaft, da sie neben einer bloßen Erleichterung im Vergleich zur persönlichen Vor-Ort-Kontrolle mit der Aussage eines fachkundigen Dritten über die Normkonformität eines Anbieters, eines Systems oder eines Dienstes einen Vertrauenstatbestand schaffen[19] und über ein Informationsdefizit bei Cloud-Kunden und Anwendern hinweghelfen soll. Dem Cloud-Kunden wird es regelmäßig an Fachkunde und Einblicken in die Unternehmensorganisation des Cloud-Anbieters mangeln. Das Zertifikat eines fachkundigen Dritten kann ihm daher mehr Sicherheit bieten, als er durch seine persönliche Vor-Ort-Kontrolle erreichen könnte.

Allerdings verlangt ein Zertifikat dem Cloud-Kunden einen Vertrauensvorschuss ab. So soll der Cloud-Kunde darauf vertrauen, dass die Aussage eines Zertifikats auch noch zu

[15] Eine Selbsteinschätzung des Cloud-Anbieters wird im Zusammenhang mit den Kontrollpflichten des Cloud-Kunden völlig zu Recht ohnehin weitgehend als unzureichend erachtet. Von einer Diskussion und Entscheidung dieser Frage wird hier aus Gründen des Platz- und Relevanzmangels Abstand genommen.
[16] BT-Drs. 16/13657, 28. So auch Art. 26 Abs. 2 aa des Entwurfs zur europäischen Datenschutzgrundverordnung (konsolidierte Fassung des Rates vom 19. Dezember 2014, „DSGVO-E“).
[17] Düsseldorfer Kreis, Orientierungshilfe, 10. Dabei betont der Arbeitskreis, dass das alleinige Vorliegen von Zertifikaten nicht von der Kontrollpflicht entbindet.
[18] So etwa WP 196, Kap. 4.2, 27.
[19] OLG Dresden, MMR 2012, 6780.

einem späteren Zeitpunkt (etwa ein Jahr später) immer noch zutrifft.[20] Tatsächlich steht die dynamische Entwicklung auf dem Gebiet der IT dabei jedoch oft im Widerspruch zur statischen Aussage einer derartigen Konformitätsbewertung. Während sich IT und Rechtswissenschaft in Wirklichkeit unaufhaltsam weiterentwickeln und sich die tatsächlichen Gegebenheiten verändern können, wird ein klassisches Zertifikat infolge einer Überprüfung in der Regel für einen festgelegten Zeitraum erteilt, z.B. zwei Jahre, und bestätigt einen möglicherweise längst vergangenen und überholten Zustand. Das Ergebnis – Unsicherheit – steht dem eigentlichen Zweck von Zertifizierungen, nämlich der Steigerung von Markvertrauen in Dienste und Dienstleister – entgegen. Unsicherheit ist eine Eigenschaft, die gerade nicht mit Zertifizierungen in Verbindung gebracht werden sollte und letzten Endes dazu führt, dass das Instrument der Zertifizierung an Reputation und Wirksamkeit verliert.[21]

3 Die dynamische Zertifizierung

Eine dynamische Zertifizierung ist ein möglicher Lösungsansatz. Sie zeichnet sich durch die kontinuierliche und automatisierte Überprüfung einzelner, zuvor festgelegter Anforderungen – insbesondere, aber nicht ausschließlich aus Datenschutz und Datensicherheit – aus. Zudem schafft sie Marktanreize[22] und zielt darauf ab, dem Cloud-Kunden die Ausübung seiner Kontrollpflicht aus § 11 Abs. 2 Satz 4 BDSG zu erleichtern.

Ein dynamisches Zertifizierungssystem erfordert ein idealerweise kontinuierliches Überwachen (Monitoring) der überprüften Systeme und Dienste mittels Messtechniken und Berechnungsmethoden (Metriken).[23] Anhand der Messergebnisse muss feststellbar sein, ob ein für die Zertifikatserteilung relevanter vorgegebener Sollwert erfüllt wird. Entscheidend ist, dass die Dynamik eines Cloud-Dienstes berücksichtigt wird. Es müssen folglich unter anderem Veränderungen rechtlicher, technischer und tatsächlicher Art bedacht werden. Das wiederum setzt voraus, dass sich die zu prüfenden Kriterien, Messergebnisse und Messtechniken während der Messung verändern können und diese Veränderungen Berücksichtigung finden. Wird ein Merkmal A zu einem Zeitpunkt X überprüft, liegt beispielsweise Dynamik vor, wenn die Prüfung des Merkmals A zu einem Zeitpunkt X+1 (der zeitlich nach X liegt) ein unterschiedliches Ergebnis erzeugt. Es können sich dabei verschiedene Konstellationen ergeben: Eine Metrik kann dazu dienen, mehrere Kriterien zu überprüfen. Ein Kriterium kann aber auch mit nur einer einzigen Metrik überprüfbar sein. Zur Darstellung desselben (rechtlichen) Kriteriums können verschiedene Metriken anwendbar sein. Und schließlich kann ein Kriterium aber

[20] *Dahm,* DuD 2002, 413 spricht insoweit von Vertrauen auf „Quasi-Kulanz" – einem (vor)vertragliches Verhalten desjenigen, der das Zertifikat verwendet.
[21] Auch nach Art. 39 Abs. 4 DSGVO-E ist die Zertifizierung bei Wegfall der Voraussetzungen zu entziehen.
[22] Hierzu *Hornung,* ZD 2014, 219 ff.
[23] Ausführlich hierzu *Stephanow/Gall*, Language Classes for Cloud Service Certification Systems, 2015 IEEE 11th World Congress on Services (SERVICES), i.E.

auch dadurch erfüllt sein, dass ein oder mehrere andere Kriterien alleine oder in Kombination anhand von einer oder mehreren Metriken alleine oder in Kombination nachgewiesen werden.

Das Vertrauen des Marktteilnehmers ist berechtigt, sobald die durch ein Zertifikat bestätigten, festgelegten Kriterien entweder innerhalb möglichst klein zu definierender Intervalle oder zu einem beliebigen Zeitpunkt bedarfsabhängig überprüfbar werden. Es wird ihm nicht abverlangt, blind auf die Zertifikatsaussage zu vertrauen, sondern ein Mittel zur Überwindung seines Informationsdefizits in die Hand gegeben. Die Werbung mit einem dynamischen Zertifikat ist damit berechtigt und lauter. Die dynamische Zertifizierung schafft folglich für die jeweiligen Teilbereiche Transparenz und Rechtssicherheit auf dem bislang undurchsichtigen Gebiet des Cloud Computing. Ziel eines dynamischen Zertifizierungskonzepts muss es demnach sein, den Prüfkatalog stets aktuell zu halten und – der Dynamik entsprechend – zu erweitern.

4 Die Methode KORA

Die Entwicklung eines dynamischen Zertifizierungssystems erfordert die Erstellung eines umfassenden Kriterienkatalogs. Hierzu bietet sich die Verwendung der Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen (KORA)[24] an. Dahinter steht die Überlegung, dass rechtliche Vorgaben in aller Regel zu abstrakt sind, um konkrete technische Gestaltungsmerkmale für ein konkretes technisches System zu enthalten.

Angesichts der gegebenenfalls unterschiedlichen Auswirkungen ist strikt zwischen Prüfungsinhalt (etwa Diensten und Systemen) und Zertifizierungsverfahren zu differenzieren.[25]

Abb. 1: Die Methode KORA

[24] Die Methode KORA wurde von der Projektgruppe verfassungsverträgliche Technikgestaltung an der Universität Kassel entwickelt. Zur Methode siehe *Hammer/Pordesch/Roßnagel*, Informatik und Gesellschaft, 1993, 21 ff.; *dies.*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten, 1993, 46 ff.

[25] Dies gründet darin, dass für beide unterschiedliche rechtliche Grundlagen gelten können.

Abbildung 1 zeigt die Methode KORA, bei der in einem vierstufigen Prüfungsaufbau rechtliche Anforderungen aus der Verfassung abgeleitet und über zwei weitere Stufen schließlich zu konkreten technischen Gestaltungsvorschlägen konkretisiert werden. Diese Vorschläge müssen zudem dynamische Aspekte betreffen,[26] kontinuierlich überwachbar[27] und schließlich automatisiert überprüfbar[28] sein.

KORA verfolgt das Ziel rechtsverträglicher und nicht „nur" rechtmäßiger Gestaltung. Rechtmäßigkeit beschreibt zwingend zu erfüllende Voraussetzungen („Muss-"Regelungen). Daneben sind „Soll-"Anforderungen solche, die in der Regel vorliegen müssen, von denen in Ausnahmefällen aber abgewichen werden kann. Rechtsverträglichkeit beschreibt einen Zustand, der erstrebenswert ist. Insoweit ist auch auf „Kann-"Regelungen zurückzugreifen, die nicht zwingend sind. Das deutsche Datenschutzrecht sieht zwingende Grundsätze vor, die einzuhalten sind. Andere Aspekte wiederum sind lediglich vorteilhaft. Auf KORA übertragen bedeutet dies, dass ein Großteil der rechtlichen Aspekte zwingend einzuhalten sein wird. Darüber hinaus sind aber auch Gestaltungsformen denkbar, die gegenüber anderen ein Mehr an Datenschutz oder -sicherheit bieten und die deshalb vorzugswürdig erscheinen. Der große Vorteil dieses methodischen Ansatzes liegt darin, dass sie dem Juristen, der normalerweise erst zu Rate gezogen wird, wenn Technik erstellt und implementiert wurde, ermöglicht, zu einem möglichst frühen Zeitpunkt gestaltend mitzuarbeiten. Ziel von KORA ist in diesem Fall, Gestaltungsvorschläge für eine datenschutzfreundliche Technik zu gewinnen.

Rechtliche Kriterien (Stufe 2) leiten sich bei KORA aus rechtlichen Anforderungen ab (Stufe 1), die wiederum direkt verfassungsrechtlichen Vorgaben (Vorstufe) entstammen, und beziehen sich einerseits auf Technik, andererseits auf soziale und rechtliche Aspekte, indem sie auf abstrakter Ebene Lösungswege für die Anforderungen aufzeigen, ohne jedoch konkrete Lösungsansätze zu benennen. Rechtlichen Kriterien kommt eine Doppelfunktion dahingehend zu, dass sie zum einen nachfolgende Konkretisierungen bewerten – und damit ein gewisses Maß an Konkretisierung erfahren haben, zum anderen liefern sie Hinweise darauf, wie eine gute Lösung aussehen muss.[29]

Technische Gestaltungsziele (Stufe 3) sind abstrakte technische Anforderungen und stellen einen Zwischenschritt zur Systematisierung technischer Gestaltung dar. Bezugspunkte von technischen Gestaltungszielen sind grundlegende Systemfunktionen, die Systemarchitektur oder aber Daten.[30] Nur selten handelt es sich dabei um zwingend einzuhaltende Aspekte.

Technische Gestaltungsempfehlungen (Stufe 4) sind das Ergebnis der Bewertung technischer Merkmale anhand der gefundenen technischen Gestaltungsziele und

[26] Andernfalls läge mangels Veränderbarkeit kein Überprüfungsbedürfnis vor.
[27] Das wäre beispielsweise nicht der Fall, wenn ein Aspekt zu einem späteren Zeitpunkt nicht mehr existiert.
[28] Gemeint ist hier ein vollständiger Automatisierungsgrad, bei dem keine menschliche Intervention nötig ist.
[29] *Hammer/Pordesch/Roßnagel*, Informatik und Gesellschaft, 1993, 21.
[30] *Pordesch,* Die elektronische Form und das Präsentationsproblem, Nomos, Baden-Baden 2003, 266.

gleichzeitig die letzte Prüfungsstufe von KORA. Angesichts der Fülle an technischen Lösungsansätzen und deren Kombinationsmöglichkeiten ist eine abschließende Betrachtung nicht möglich. Eine Sammlung von Gestaltungsvorschlägen kann demnach lediglich eine stark begrenzte Auswahl darstellen und erhebt keinen Anspruch auf Vollständigkeit.

5 KORA am Beispiel „Verfügbarkeit“

Verfügbarkeit ist ein rechtliches Kriterium (Stufe 2). Es folgt für den Prüfungsinhalt aus den Anforderungen Datenschutz und Geheimnisschutz (Stufe 1), die wiederum auf den Grundrechten auf informationelle Selbstbestimmung beziehungsweise auf Eigentum und auf Berufsfreiheit (Vorstufe) basieren. Verfügbarkeit als eines der IT-Sicherheitsziele[31] gehört sinnvollerweise zu einem umfassenden Datenschutzsystem. Es soll Informationen vor Verlust, Entzug, Blockade und Zerstörung schützen und gleichzeitig (in seiner zweiten Ausprägung) dafür sorgen, dass ein System bei autorisiertem Zugriff innerhalb einer bestimmten Zeit zur Verfügung steht und technisch vor der Beeinträchtigung der Verfügbarkeit durch Nichtberechtigte geschützt ist. Dem Cloud-Kunden müssen folglich die Cloud-Dienste sowie die Daten zu jeder Zeit in dem vertraglich vereinbarten Umfang zur Nutzung zur Verfügung stehen. Obgleich es sich bei der Verfügbarkeit um ein IT-Sicherheitsziel handelt, richten sich die Voraussetzungen und die Rechtsfolgen nach vertraglich zwischen dem Cloud-Anbieter und dem Cloud-Kunden zu vereinbarenden Erfüllungsgraden (Service Levels). Die Möglichkeit des Zugriffs auf Cloud-Ressourcen über ein öffentliches Netzwerk, wie etwa bei der Public Cloud, und die damit verbundenen erhöhten Gefahren stellt den Cloud-Anbieter in diesem Zusammenhang vor eine große Herausforderung. Fehlerhafte Systemkonfigurationen und eine große Anzahl an Cloud-Serviceanfragen können der Verfügbarkeit (sowohl der Daten als auch der Systeme) abträglich sein. Strafrechtlich kann ein Angriff auf die Verfügbarkeit beispielsweise über § 265a StGB (Erschleichung von Leistungen) oder § 303a StGB (Datenveränderung) von Bedeutung sein.

„Verfügbarkeit“ ist für das Cloud Computing (den Prüfungsinhalt) von hervorgehobener Bedeutung. Es tritt in zwei verschiedenen Formen auf. Zum einen bezieht es sich auf Daten, zum anderen auf Systeme.[32] Hier wird das Kriterium „Verfügbarkeit“ in Bezug auf Daten besprochen. Dabei kann es vorkommen, dass Gestaltungsziele (Stufe 3) oder -vorschläge (Stufe 4) auf beide Erscheinungsformen anwendbar sind.[33]

Die Anwendung von KORA stellt sich für das hier darzustellende Beispiel „Verfügbarkeit“ bezüglich des zu zertifizierenden Inhalts (Cloud-Dienst) wie folgt dar.

[31] § 2 Abs. 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.
[32] Wie es Gegenstand des Entwurfs des IT-Sicherheitsgesetzes (BT-Drks. 18/4096) ist.
[33] So schützt beispielsweise die Ausfallsicherheit in erster Linie die Verfügbarkeit von Systemen, ohne letztere, wären allerdings auch keine Daten verfügbar, so dass das Gestaltungsziel auch für die Verfügbarkeit von Daten relevant ist.

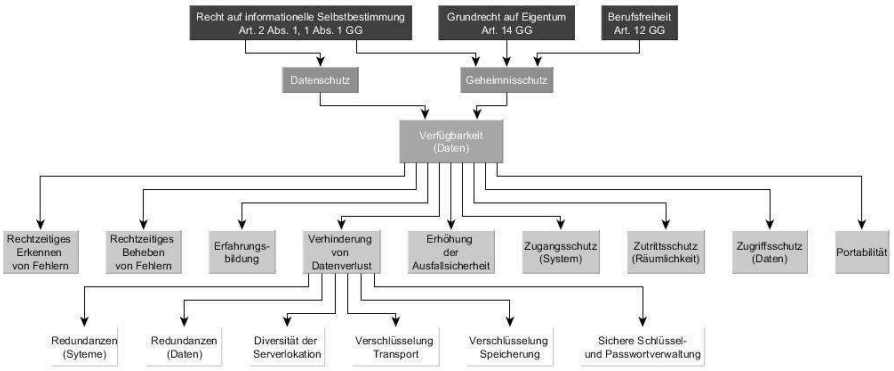

Abb. 2: Die Methode KORA am Beispiel „Verfügbarkeit“ für den Prüfungsinhalt

Hinweis: Abbildung 2 zeigt die Anwendung der Methode KORA auf das Beispiel der Verfügbarkeit (Stufe 2) bezogen auf den Prüfungsinhalt. Während die verfassungsrechtlichen Grundlagen (Vorstufe) sowie die zugrundeliegenden rechtlichen Anforderungen (Stufe 1) abschließend sind, kann dies für die aus dem Kriterium der Verfügbarkeit abzuleitenden technischen Gestaltungsziele (Stufe 3) und Gestaltungsvorschläge (Stufe 4) nicht gelten. Vielmehr wurde die Konkretisierung des Kriteriums „Verfügbarkeit“ aus Gründen der Übersichtlichkeit auf neun Gestaltungsziele beschränkt. Davon wurde – wiederum exemplarisch – lediglich jenes der „Verhinderung von Datenverlust“ zu sechs (nicht abschließenden) Gestaltungsvorschlägen konkretisiert.

Aus dem rechtlichen Kriterium der Verfügbarkeit (gegebenenfalls in Verbindung mit zusätzlichen Kriterien, wie etwa denjenigen der Integrität der Daten und Systeme, der Transparenz, der Überprüfbarkeit, der Beherrschbarkeit und Steuerungsfähigkeit, der Beweissicherung) lassen sich unter anderem die technischen Gestaltungsziele „rechtzeitiges Erkennen von Fehlern“, „rechtzeitiges Beheben von Fehlern“, „Erfahrungsbildung“, „Verhinderung von Datenverlust“, „Erhöhung der Ausfallsicherheit“, „Zugangsschutz“, „Zutrittsschutz“, „Zugriffsschutz“ und „Portabilität“ ableiten.

Während sich die ersten beiden Ziele von selbst erklären, ist mit „Erfahrungsbildung“ gemeint, dass beispielsweise gezielte Angriffe auf Systeme einen Lerneffekt erzielen, der Verfügbarkeit unterstützen kann. Zur „Verhinderung von Datenverlust“ sogleich. „Erhöhung der Ausfallsicherheit“ kann beispielsweise durch physische Serversicherungsmaßnahmen erfolgen. „Zugangsschutz“ bezieht sich auf Systeme, „Zutrittsschutz“ auf Räumlichkeiten und „Zugriffsschutz“ auf Daten. Gemeint ist jeweils Schutz vor unberechtigtem Zugang, Zutritt und Zugriff. „Portabilität“ betrifft Daten und die Möglichkeit deren Verlagerung von einem Cloud-Anbieter zu einem anderen. Offene Schnittstellen und Datenformate können einen sog. Vendor-lock in verhindern, der dadurch entsteht, dass ein Cloud-Anbieter beispielsweise unübliche Formate verwendet, die nicht mit den Systemen anderer Anbieter kompatibel sind und damit verhindert oder

erschwert, dass ein Cloud-Kunde zu einem anderen Anbieter wechselt.

Das Gestaltungsziel „Verhinderung von Datenverlust“ wurde exemplarisch weiter zu sechs nicht abschließenden Gestaltungsvorschlägen konkretisiert. Dies sind namentlich „Redundanzen“ – jeweils von Systemen und Daten, „Diversität der Serverlokation“, „Verschlüsselung“ – jeweils auf dem Transport und während der Speicherung und die „sichere Schlüssel- und Passwortverwaltung“.

Verfügbarkeit sollte dadurch gefördert werden, dass Systeme und Daten jeweils redundant vorgehalten werden. Es werden dabei von Daten beispielsweise Kopien angefertigt, die verhindern sollen, dass die Daten durch einen Vorfall unwiederbringlich gelöscht werden. Verteilen sich die Systeme und die darin gespeicherten Daten zudem auf verschiedene Serverstandorte, ist gleichzeitig die Gefahr verringert, die beispielsweise von Naturkatastrophen für die Daten und Systeme ausgeht („Diversität der Serverlokation“). Daten müssen zudem auf dem Transport ebenso wie bei deren Speicherung „in der Cloud“ dem jeweiligen Stand der Technik entsprechend verschlüsselt werden. Schließlich sind die Schlüssel und Passwörter sicher zu verwalten.

Wie bereits erwähnt, handelt es sich hierbei um eine nicht abschließende, exemplarische Ableitung. Ziel war es, das methodische Vorgehen zu veranschaulichen. Hinsichtlich des analysierten Beispiels „Verfügbarkeit“ in Bezug auf den Prüfungsinhalt unterscheidet sich die dynamische freilich nicht von der statischen Zertifizierung. Beide haben die Bestätigung der Normkonformität von Cloud-Diensten zum Gegenstand. Die Betrachtung von „Verfügbarkeit“ im Zusammenhang mit dem dynamischen Verfahren wird zwar in weiten Teilen mit den hier dargestellten Ableitungen zum Inhalt übereinstimmen, darüber hinaus aber auch Unterschiede aufweisen. Diese Unterschiede rühren daher, dass nach bisherigem Erkenntnisstand die Daten, deren Übermittlung an den Zertifizierer zum Zwecke der dynamischen Zertifizierung erforderlich ist, keine personenbezogenen Daten im Sinne des Bundesdatenschutzgesetzes sind. Solche sind aber erforderlich damit letzteres Anwendung findet. Gemäß § 3 Abs. 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ Die im Rahmen eines dynamischen Zertifizierungsverfahrens zu übermittelnden Daten beziehen sich jedoch aller Voraussicht nach nicht auf natürliche Personen. Es handelt sich vielmehr um Prozess- und Organisationsdaten aus dem Unternehmen des Cloud-Anbieters. Jedenfalls weisen sie für den Zertifizierer keinen Personenbezug auf. Selbst für den Fall, dass die Übermittlung von Daten, die aus Sicht des Zertifizierers den Rückschluss auf bestimmte oder bestimmbare Personen (etwa einen Mitarbeiter des Cloud-Anbieters) zulassen, nicht ausgeschlossen werden kann, wird Kenntnis des Zertifizierers dieser Daten voraussichtlich nicht erforderlich sein. Vielmehr sind diese Daten vor ihrer Übermittlung an den Zertifizierer zu anonymisieren. Demzufolge ist das Bundesdatenschutzgesetz insoweit nicht anwendbar. Daraus folgt für das rechtliche Kriterium der Verfügbarkeit, dass es sich für das dynamische Zertifizierungsverfahren aus der Anforderung „Datenschutz“ nur indirekt und zwar insoweit ableitet, dass der zu zertifizierende Cloud-Dienst selbst datenschutzgerecht ausgestaltet sein muss. Hingegen folgt Verfügbarkeit in

Bezug auf das Verfahren vorrangig aus den Anforderungen „Geheimnisschutz", „Nachvollziehbarkeit und Kontrollierbarkeit der Zertifizierung" und „unternehmerische Entscheidungsfreiheit". Der Aspekt der Dynamik spiegelt sich daneben in den Kriterien „Überprüfbarkeit",[34] „Veränderbarkeit",[35] „Adäquanz"[36] und „Aktualität"[37] wider, die sich wiederum aus den Anforderungen „Rechtssicherheit", „Nachvollziehbarkeit" und „Kontrollierbarkeit der Zertifizierung" sowie „Verbraucherschutz" ableiten. Das dynamische Zertifizierungsverfahren muss hinsichtlich Aufbau und Organisation, Rechtsfolgen und Voraussetzungen, Kompetenzen und Haftung transparent sein. Die Prüfungsergebnisse müssen verfügbar sein – für welchen Adressatenkreis, bleibt zu untersuchen. Klar ist indes, dass ein dynamisches Zertifizierungsverfahren, dessen Ergebnisse nicht jederzeit abrufbar sind, nicht den vollständigen Mehrwert gegenüber einem statischen Verfahren entfalten kann. Denn nur durch Verfügbarkeit der Prüfungsergebnisse und der zugrundeliegenden Richtlinien kann Vertrauen in das dynamische Zertifikat und damit in den zertifizierten Dienst gewonnen werden. Anwender und Cloud-Kunde müssen in Erfahrung bringen können, was die dynamische Prüfung ergeben und anhand welcher Regeln sie stattgefunden hat. Gleiches gilt für die Verfügbarkeit von Systemen. Nur wenn die für die dynamische Zertifizierung erforderlichen Systeme verfügbar sind, kann eine automatisierte dynamische Überprüfung überhaupt stattfinden.

Auf der Ebene der technischen Gestaltungsziele erlangen von den oben für den Inhalt abgeleiteten Zielen insbesondere all diejenigen besondere Bedeutung für das Zertifizierungsverfahren, die Aspekte der Dynamik und des Lernprozesses widerspiegeln. Das sind insbesondere die rechtzeitige Fehlererkennung und -behebung sowie die Erfahrungsbildung.

Ein dynamisches Zertifizierungsverfahren erfordert eine abschließende Betrachtung und Beurteilung aller rechtlichen Vorgaben. In einem weiteren Schritt sind die einzelnen Vorschläge im interdisziplinären Diskurs auf ihre Wirtschaftlichkeit und Funktionalität hin zu untersuchen. Nur so kann überhaupt ein rechtmäßiges, wirtschaftliches und technisch umsetzbares System entstehen, das sich von vorhandenen Verfahren absetzt.

[34] Die Durchführung einer Überprüfungsmaßnahme erfordert Überprüfbarkeit. Der Einzelne muss die Prüfungsschritte nachvollziehen können, um darüber zu entscheiden, ob er dagegen vorgehen will oder nicht.

[35] Hier wird der Unterschied der dynamischen zur statischen Zertifizierung besonders deutlich. Das Kriterium beinhaltet Dynamik und bezieht sich gleichfalls auf rechtliche, technische und tatsächliche Gegebenheiten. Das dynamische Zertifizierungsverfahren muss anpassbar, das heißt grundsätzlich offen für Neuerungen sein.

[36] „Adäquanz" wird hier im Sinne einer generellen Geeignetheit begriffen. Die einzelnen Komponenten des dynamischen Zertifizierungsverfahrens müssen so ausgewählt sein, dass eine Förderung der angestrebten dynamischen Gestaltung dadurch nicht außerhalb aller Wahrscheinlichkeit liegt. „Veränderbarkeit" ist dabei notwendige Bedingung für „Adäquanz". Im Unterschied zu ersterer, geht es bei Adäquanz statt um die bloße Möglichkeit der Berücksichtigung der Dynamik um eine entsprechende Wahrscheinlichkeit. „Adäquanz" kommt in mehrfacher Hinsicht Bedeutung zu, namentlich für die verwendete Technik und die Organisation.

[37] Eng verwoben mit „Adäquanz" und von herausragender Bedeutung ist das Kriterium der Aktualität. Dieses Alleinstellungsmerkmal gegenüber herkömmlichen Zertifizierungssystemen ist durch eine stetige Anpassung der Prüfanforderungen an die rechtlichen, tatsächlichen und technischen Gegebenheiten, eine Aktualisierung der verwendeten Systeme und Prozesse und der Überprüfung des Sachverstands und der Unabhängigkeit der eingesetzten Prüfungspersonen sicherzustellen.