Verbundsabschlussbericht

AUDITOR

European Cloud Service Data Protection Certification

Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Vorgelegt durch:

Prof. Dr. Ali Sunyaev, Dr. Sebastian Lins, Heiner Teigeler
Karlsruher Institut für Technologie

Laufzeit des Vorhabens: 01.11.2017 – 30.04.2024

doi: 10.5445/IR/1000175491

Verbundsabschlussbericht

Vorhabensbezeichnung: European Cloud Service Data Protection Certification (AUDITOR)	**Förderkennzeichen:** 01MT17003
Projektleiter: Prof. Dr. Ali Sunyaev	Tel.: 0 721 608-46037 Fax: 0 721 608-46581 E-Mail: sunyaev@kit.edu
Laufzeit des Vorhabens: 01.11.2017 – 30.04.2024	
Projektpartner: 1. Karlsruher Institut für Technologie 2. Universität Kassel 3. Datenschutz cert GmbH 4. eco e.V. 5. ecsec GmbH 6. Cloud&Heat GmbH 7. DIN e.V. Mit der Unterstützung von TrustedCloud, Hornetsecurity und VOICE-Bundesverband der IT-Anwender sowie weiteren assoziierten Partnern ohne Förderung	
Zitation Sunyaev, Ali, Lins, Sebastian, & Teigeler, Heiner (2024). AUDITOR: European Cloud Service Data Protection Certification – Verbundsabschlussbericht. doi: 10.5445/IR/1000175491	
Alle zentralen Ergebnisdokumente sind auf der Website des Projektes (www.auditor-cert.de) und des Programmeigners Trusted Cloud (https://www.trusted-cloud.de/dsgvo-zertifikat.html) der Öffentlichkeit zugänglich gemacht.	

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs. – Absatz
Art. – Artikel
AUDITOR – European Cloud Service Data Protection Certification
BDSG – Bundesdatenschutzgesetz
BfDI – Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMBF – Bundesministerium für Bildung und Forschung
BMI – Bundesministerium des Innern
BMWK – Bundesministerium für Wirtschaft und Klimaschutz
BSI – Bundesamt für Sicherheit in der Informationstechnik
C5 – Cloud Computing Compliance Controls Catalogue
CSA – Cloud Security Alliance
DAkkS – Deutsche Akkreditierungsstelle
DIN – Deutsche Institut für Normung e. V.
DIN SPEC – DIN Spezifikation
DSGVO – Datenschutz-Grundverordnung (Geltung ab 25.5.18)
DSK – Datenschutzkonferenz
EDSA – Europäischer Datenschutzausschuss
ENISA – Agentur der Europäischen Union für Cybersicherheit
ESCloud – European Secure Cloud Label
KBP – Konformitätsbewertungsprogramm
KIT – Karlsruher Institut für Technologie
KMU – Kleine und mittelständische Unternehmen
KORA – Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen
LDI NRW – Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfD – Landesbeauftragte:r für den Datenschutz
NGCert – Next Generation Certification
Nr. – Nummer
TCDP – Trusted Cloud Datenschutz-Profil
ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

1. Kurzdarstellung des Projektes

1.1. Aufgabenstellung

1.1.1. Problemstellung

In den letzten Jahrzehnten hat ein technologischer Paradigmenwechsel vom Kauf und eigenständigen Betrieb der Soft- und Hardware hin zum Beziehen der Ressourcen über den Cloud-Dienst-Markt die Flexibilität und Kosteneffizienz von IT-Abteilungen gesteigert. Dadurch konnte die Wettbewerbsfähigkeit besonders von kleinen und mittelständischen Unternehmen (KMU) erhöht werden, da sich diese durch den Einsatz von Cloud-Diensten auf ihr Kerngeschäft fokussieren und somit die Entwicklung interner IT-Strukturen vernachlässigen können. Trotz der zahlreichen Vorteile von Cloud-Diensten bestehen durch den möglichen Verlust der Kontrolle über die Prozesse und Daten weiterhin Bedenken. Nicht nur Kontrollverlust, sondern auch mangelnde Transparenz wirken sich insbesondere dort negativ aus, wo zum Beispiel besonders sensible Daten verarbeitet werden und Geheimhaltungspflichten Berufsgeheimnisträger besonders verpflichten. Erste Zertifizierungen von Cloud-Diensten haben bereits die Transparenz erhöht und geholfen dem Kontrollverlust entgegenzuwirken. Dabei ist es für die Zukunftsfähigkeit und Vertrauenswürdigkeit einer Zertifizierung unabdinglich, dass sie geltenden Gesetzen und einschlägigen Regularien entspricht. Im Cloud-Kontext ist aus rechtlicher Sicht insbesondere die im Mai 2016 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) von Relevanz. Während die Zertifizierung nach dem Bundesdatenschutzgesetz (BDSG, a. F.) in dem Pilotprojekt „Datenschutzzertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte „Trusted Cloud Datenschutz-Profil“ (TCDP) untersucht wurde, ergab sich aufgrund vielfältiger Entwicklungen weiterer Handlungsbedarf. So konnten bei der Entwicklung der TCDP-Zertifizierungskriterien noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke (zum Beispiel Cloud Computing Compliance Controls Catalogue (C5) und European Secure Cloud Label (ESCloud)) und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden. Es ergab sich somit eine dringende Notwendigkeit das TCDP aufgrund des Anwendungsvorrangs des EU-Rechts an die veränderte Rechtslage mit einer klaren Ausrichtung an den europäischen Markt anzupassen. Das Forschungsprojekt „AUDITOR“ *(European Cloud Service Data Protection Certification)* wurde vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert, um Klarheit und mehr Rechtssicherheit in dieser Ausgangslage zu schaffen.

1.1.2. Zielsetzung

Ziel von AUDITOR war die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten. Eine Datenschutzzertifizierung soll insbesondere KMU helfen, bekannte Probleme zu adressieren, Transparenz zu schaffen und bei der Auftragsverarbeitung Rechtssicherheit auf einer europäischen Ebene zu vermitteln. Um eine nachhaltige Datenschutzzertifizierung zu konzipieren, wurde zunächst ein

Kriterienkatalog für die Zertifizierung von Cloud-Diensten nach der Datenschutz-Grundverordnung entwickelt (Teilziel 1). Hierbei wurden Zertifizierungskriterien insbesondere aus den Vorgaben der Datenschutz-Grundverordnung und den einschlägigen Normen im Bereich Datenschutz, Datensicherheit und Privatsphäre abgeleitet, klassifiziert und damit ein umfassender AUDITOR-Kriterienkatalog entwickelt und fortlaufend multi-perspektivisch evaluiert. Außerdem wurde ein geeignetes Zertifizierungsverfahren zur Durchführung einer anerkannten Datenschutzzertifizierung konzipiert und in einem Konformitätsbewertungsprogramm (KBP) für die Akkreditierung formuliert (Teilziel 2). Wichtig waren hierbei insbesondere die Spezifikation von modularen Zertifizierungsprozessen und die Anerkennung bestehender Zertifikate. Das entwickelte Zertifizierungsverfahren und die im AUDITOR-Projekt erarbeiteten und für eine Standardisierung vorbereiteten Kriterien wurden in drei Pilotierungen bei Cloud-Anbietern erprobt und validiert (Teilziel 3). Das Zertifizierungsverfahren hat anschließend erfolgreich den formalen Bewilligungsprozess von Zertifizierungen nach Art. 42 DSGVO durchlaufen (Teilziel 4). Diese Ziele wurden durch fortlaufende Öffentlichkeitsarbeit, Zusammenarbeit mit anderen Stellen sowie Standardisierungsaktivitäten unterstützt (Teilziel 5).

1.2. Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das AUDITOR-Projekt konnte auf der einen Seite auf bestehende Zertifizierungen und Forschung zur Cloud-Service-Zertifizierung zurückgreifen. Auf der anderen Seite stellte die AUDITOR-Zertifizierung eine der ersten Bemühungen dar, eine Datenschutzzertifizierung gemäß Art. 42 DSGVO zu entwickeln, sodass viele Unsicherheiten und offene Diskussionspunkte überwunden werden mussten.

Zunächst konnte auf die Vorarbeiten des TCDP aufgebaut werden. Das TCDP stellte eine Zertifizierung nach dem alten Bundesdatenschutzgesetz dar und wurde im Pilotprojekt „Datenschutzzertifizierung für Cloud-Dienste“ im September 2016 finalisierst. Die Entwicklung des TCDP wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (heute BMWK) gefördert und stand zur freien Verwendung bereit, und konnte somit als Grundlage für AUDITOR ganzheitlich herangezogen werden. Da bei der Entwicklung der Zertifizierungskriterien vom TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. C5 des Bundesamts für Sicherheit in der Informationstechnik (BSI) – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, musste mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25. Mai 2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies wurde zunächst im AUDITOR-Kriterienkatalog durchgeführt, welcher alle relevanten Vorschriften für die Datenschutzzertifizierung von Cloud-Diensten in der Datenschutz-Grundverordnung zu prüffähigen Kriterien konkretisiert.

Auf der anderen Seite war das Projekt mit fortlaufenden Veränderungen sowie vielen Unsicherheiten in Bezug auf die Umsetzung der Anforderungen der Datenschutz-Grundverordnung und konkrete Fragen der Zertifizierung von Datenverarbeitungsvorgängen und der Akkreditierung von Zertifizierungsverfahren konfrontiert. So wurden während der gesamten Projektlaufzeit auf nationaler und europäischer Ebene Leitlinien, Empfehlungen und Umsetzungshinweise zu datenschutzrechtlichen

Anforderungen, die Auswirkungen auf die Zertifizierung und Akkreditierung haben, entwickelt, überarbeitet, oder miteinander harmonisiert. Das AUDITOR-Konsortium hat daher bereits zu Beginn eine fortlaufende Marktbeobachtung durchgeführt. Dabei hat sich gerade in der zweiten Projekthälfte gezeigt, dass einige wesentliche Änderungen und teilweise unerwartete Ereignisse auch maßgeblichen Einfluss auf das AUDITOR-Projekt und seine Ergebnisse hatten. Hierzu zählen auf nationaler Ebene mehrere Papiere der Datenschutzkonferenz (DSK) und auf europäischer Ebene Leitlinien und Empfehlungen des europäischen Datenschutzausschusses (EDSA), welche neu veröffentlicht oder überarbeitet wurden. Diese haben jeweils neue oder geänderte Anforderungen an die Datenschutzzertifizierungen oder Akkreditierung gestellt und mussten entsprechend nachträglich berücksichtigt werden.

Darüber hinaus kommt es immer wieder zu neuen Entscheidungen in der Rechtsprechung, die nicht nur Auslegungsfragen der Datenschutz-Grundverordnung betreffen, welche relevant für das Projekt sind, sondern auch neue Anforderungen an einzelne Themen stellen, die im AUDITOR-Kriterienkatalog abgebildet sind, wodurch Kriterien umfänglich überarbeitet werden mussten. Dies betrifft insbesondere das „Schrems II-Urteil“ des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten an Drittländer, das die Übermittlung personenbezogener Daten in die USA auf Grundlage des Privacy – Shield-Abkommens für unwirksam erklärt. Eine Übermittlung in Drittländer wie die USA ist jedoch gerade im Cloud-Kontext üblich, sodass das Urteil auch einen maßgeblichen Einfluss auf den AUDITOR-Kriterienkatalog hatte. Zu den weiteren Bestrebungen am Markt mit direktem Einfluss auf AUDITOR zählt auch die Schaffung von IT-Sicherheitszertifizierungen durch den EU Cybersecurity Act, sodass bspw. die Agentur der Europäischen Union für Cybersicherheit (ENISA) einen ersten Entwurf einer Cybersecurity Zertifizierung für Cloud-Dienste entwickelt hatte, welcher mit der AUDITOR-Zertifizierung abgeglichen werden musste, um eine gegenseitige Anerkennung und europaweite Kompatibilität zwischen dem Datenschutz und der IT-Sicherheit zu gewährleisten. Diese Marktentwicklungen und Ereignisse führten dazu, dass das AUDITOR-Zertifizierungsverfahren angepasst werden musste.

Besonders hervorzuheben sei auch, dass jede Datenschutzzertifizierung einen Bewilligungsprozess durchlaufen muss. Zu Projektbeginn war dieser Prozess noch nicht spezifiziert. AUDITOR war gemeinsam mit EuroPriSe das erste Zertifizierungsverfahren, welches den Bewilligungsprozess in Deutschland durchlaufen hat. Es resultierten immer wieder Verzögerungen durch Diskussionen und Unklarheiten beim Bewilligungsprozess, insb. wegen seiner Neuheit sowie unklarer Prozessschritte und Verantwortlichkeiten.

1.3. Planung und Ablauf des Vorhabens

Die Ziele des Forschungsprojekts AUDITOR lassen sich in vier wesentliche Säulen unterteilen (siehe Abbildung 1): 1) Entwicklung des Kriterienkatalogs; 2) Entwicklung des KBP; 3) Sicherstellung der Nachhaltigkeit und Überführung in die Praxis; sowie 4) fortlaufende Erprobung des Verfahrens. Die entsprechenden Arbeiten wurden iterativ und teilweise parallel durchgeführt. Im Folgenden wird die zeitliche Entwicklung des Kriterienkatalogs und des KBPs sowie deren Bewilligung skizziert.

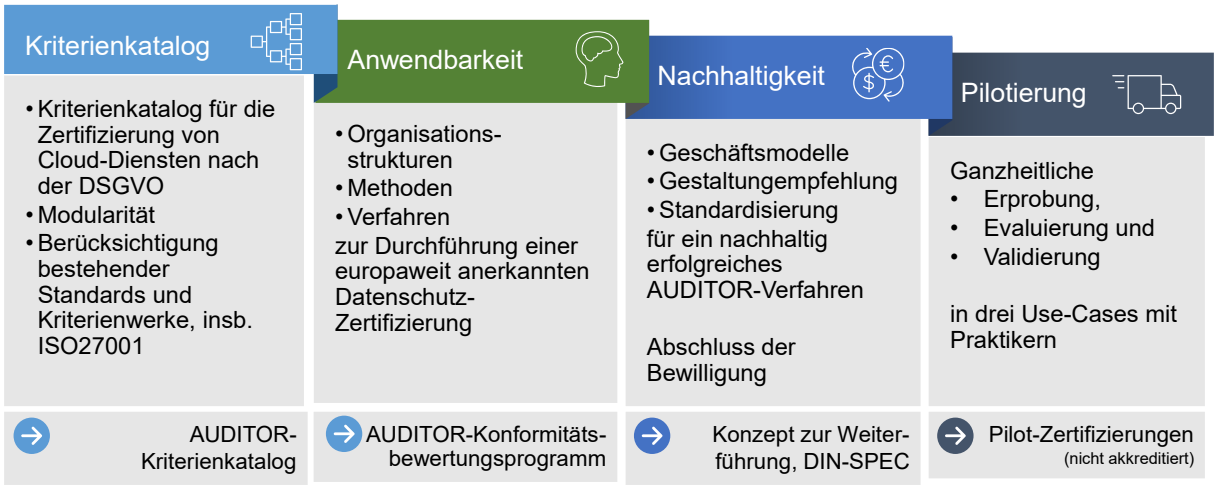

Abbildung 1. Schematische Darstellung der Meilensteine des AUDITOR-Projekts.

1.3.1. Ablauf zur (Weiter-)Entwicklung des Kriterienkatalogs

Zur Entwicklung des Kriterienkatalogs wurde eine iterative Vorgehensweise angewandt, welche nicht nur die vielen Perspektiven des Projektkonsortiums vereint, sondern gerade auch zentrale Akteure im Themenfeld der Datenschutzzertifizierung einschließt. Insbesondere diese frühzeitige und konsequente Einbindung verschiedener Stakeholder am Markt (darunter Projektpartner und assoziierte Partner sowie Datenschutz-Aufsichtsbehörden) ermöglichte die fortlaufende kritische Begutachtung des Kriterienkatalogs.

Zusammengefasst lässt sich die Entwicklungshistorie des Kriterienkatalogs wie folgt skizzieren (Abbildung 2):

- Kriterienkatalog v 0.1 (Beginn November 2018)
  - Übernahme und kritische Reflektion des TCDP-Kriterienkatalogs.
  - Intensive Überarbeitung und Ergänzung gemäß den Anforderungen der Datenschutz-Grundverordnung.
- Kriterienkatalog v 0.2
  - Gemeinsame Überarbeitung und insb. Ergänzung der Umsetzungshinweise und Nachweise.
- Kriterienkatalog v 0.3
  - Gemeinsame kritische Reflektion und Nachbearbeitung des Kriterienkatalogs.
- Kriterienkatalog v 0.4
  - Interne Diskussion des Kriterienkatalogs innerhalb des Projektkonsortiums.
  - Umsetzung der Änderungen aufgrund vorangegangener Diskussionen.
- Kriterienkatalog v 0.5
  - Ganztägiger Workshop zur Diskussion des Kriterienkatalogs in Kassel. Teilnehmer waren Vertreter der Aufsichtsbehörden, darunter Vertreter des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), des Landesbeauftragten für den Datenschutz (LfD) Niedersachen, des LfDI Mecklenburg-Vorpommern, des Bundesbeauftragten für den Datenschutz und

die Informationsfreiheit (BfDI) sowie Vertreter der Deutschen Akkreditierungsstelle (DAkkS), EuroCloud, TrustedCloud, datenschutz cert, das Deutsche Institut für Normung e. V. (DIN), KIT und der Universität Kassel.
    - Zudem hat das BSI die Fassung des Kriterienkatalogs kommentiert, insbesondere hinsichtlich der Sicherheitsanforderungen.
- Kriterienkatalog v 0.6
    - Vorstellung und Diskussion des Kriterienkatalogs auf einem großen Projekttreffen in Karlsruhe am 23.03.2018 mit allen Projektpartnern und Interessierten.
    - Einarbeitung des Feedbacks und Überarbeitung.
- Kriterienkatalog v 0.7
    - Vorstellung des AUDITOR-Kriterienkatalogs im Rahmen eines presseöffentlichen Fachgesprächs beim BMWK am 06.06.2018 in Berlin.
    - Diskussion des Kriterienkatalogs im Rahmen des Workshops zur Umsetzung der Datenschutzzertifizierung AUDITOR am 12.07.2018 in Köln.
    - Einarbeitung des Feedbacks aus Fachgespräch und Workshop.
- Kriterienkatalog v 0.8
    - Diskussion des Kriterienkatalogs im Rahmen des Workshops zur Umsetzung und Prüfung der Datenschutzzertifizierung am 15.11.2018 in Berlin.
    - Große interne Diskussionsrunde zum Kriterienkatalog im Rahmen des AUDITOR-Projekttreffens am 06.11.2018 in Frankfurt.
    - Überarbeitung anhand des Feedbacks; insb. Ergänzung des Kriterienkatalogs um Kriterien an Cloud-Anbieter als Verantwortliche von Datenverarbeitungsvorgängen.
- Kriterienkatalog v 0.9
    - Vorstellung und Diskussion des Kriterienkatalogs im Rahmen des internationalen AUDITOR-Workshops am 11.04.2019 in Brüssel.
    - Einarbeitung diversen Feedbacks von assoziierten Partnern.
    - Finale Fassung des Kriterienkatalogs bildete Grundlage für die Pilotierung.
- Kriterienkatalog v 0.99
    - Einarbeitung Feedback vom Treffen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) am 17.06.2019 in Düsseldorf, insb. Einteilung der Umsetzungshinweise nach Schutzklassen.
    - Einarbeitung diversen Feedbacks von assoziierten Partnern.
    - Anpassung der Rubrik „Nachweise“ gemäß der Ermittlungsmethoden zur Schaffung von Transparenz und Nachvollziehbarkeit.
    - Anpassung der Rubrik „Umsetzungshinweise“ aus den Ergebnissen der Pilotierungen, um weitere Umsetzungshinweise gemäß den Feststellungen zur Umsetzung der Kriterien bei Pilotpartnern zu ergänzen. Zudem wurden Verweise auf die neue ISO/IEC 27701 zu Datenschutzmanagementsystemen ergänzt.
    - Einarbeitung Lessons Learned der Pilotierungen.

- Dieser Kriterienkatalog wurde zur Prüfung der Akkreditierungsfähigkeit bei der DAkkS am 04.02.2020 eingereicht.

- Kriterienkatalog v 0.99f
  - Der Kriterienkatalog wurde im Rahmen der nationalen Bewilligung fortlaufend weiterentwickelt. Einerseits aufgrund der Änderungswünsche durch die DAkkS aber insbesondere durch die Datenschutz-Aufsichtsbehörde von NRW.
  - Änderungen betrafen insb. Kriterien zum Drittlandtransfer.
  - Zudem hat die DSK am 16.04.2021 ihr verpflichtendes Papier zu „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ veröffentlicht. Dort werden weitere Anforderungen an Zertifizierungsverfahren gestellt, welche vom AUDITOR-Konsortium umgesetzt wurden.
- Kriterienkatalog v 1.0
  - Am 17.04.2024 hat der EDSA seine Stellungnahme (‚Opinion‘) zum AUDITOR-Kriterienkatalog formal abgegeben.
  - Die Änderungsempfehlungen wurden vom Konsortium umgesetzt.
  - Am 28.06.2024 hat das LDI NRW die Kriterien formal genehmigt. Die DAkkS führt seit dem 10.09.2024 AUDITOR als Zertifizierungsverfahren auf. Damit ist das Bewilligungsprozess formal erfolgreich abgeschlossen.

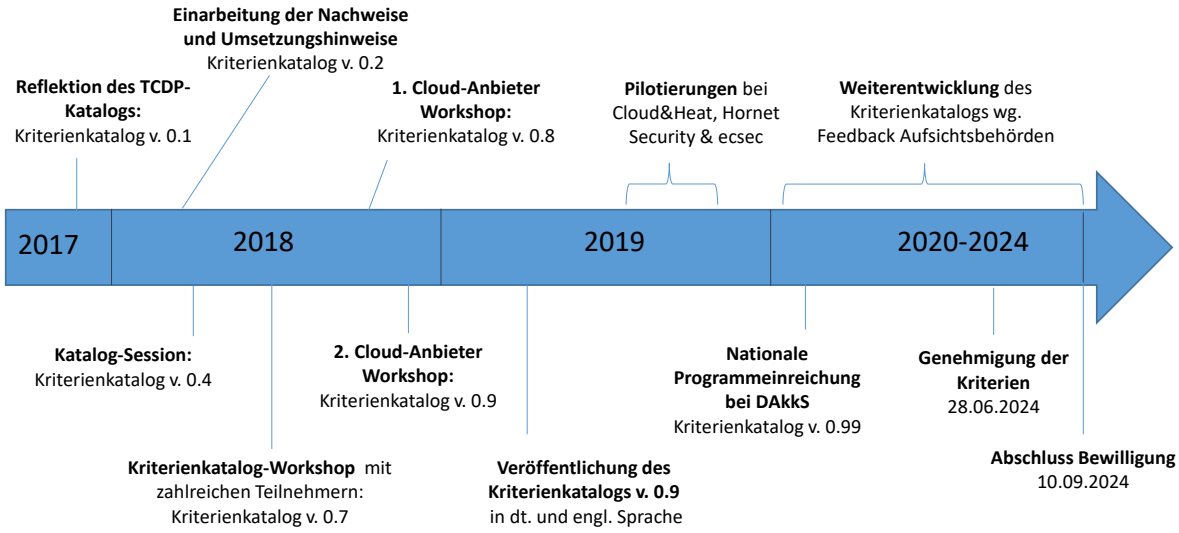

Abbildung 2. Übersicht über die Entwicklungshistorie des AUDITOR-Kriterienkatalogs.

1.3.2. Ablauf zur (Weiter-)Entwicklung des Konformitätsbewertungsprogramms

Parallel zur Entwicklung und Verbesserung des Kriterienkatalogs wurde das KBP erstellt und fortlaufend überarbeitet. Für die Erstellung des KBP hat sich das Konsortium zunächst in die relevanten ISO-Normen eingearbeitet, darunter bspw. DIN EN ISO/IEC 17000/07/21/25/65/67, sowie alle weiteren relevanten Vorgaben studiert, wie bspw. die DAkkS-Regel 71 SD 0 016. Aufbauend auf der

Verfahrensordnung des TCDP wurde ein erster Entwurf des KBP erstellt. Dieser wurde anschließend mit den Projektpartnern gemeinsam evaluiert und verbessert.

Am 29.08.2018 hat das AUDITOR-Konsortium in Kassel einen Workshop mit der DAkkS durchgeführt, um den aktuellen Stand des KBP gemeinsam zu besprechen, offene Probleme zu identifizieren, und die weiteren Schritte zu planen. Dabei konnte bereits festgestellt werden, dass das KBP einen hohen Reifegrad erreicht hat. Basierend auf dem Feedback des Workshops wurde das KBP überarbeitet und insbesondere Prüfmethoden gemeinsam im Konsortium für jedes Kriterium spezifiziert und in einem Begleitdokument zum Kriterienkatalog festgehalten.

Im Dezember 2018 wurde die Entwurfsfassung 0.3 des KBP an die DAkkS zur Begutachtung übermittelt. Das Feedback ist im Januar 2019 eingetroffen und forderte nur geringfügige Änderungen am KBP.

Die Durchführung der Pilotierungen hat auch zu Veränderungen am KBP geführt. Dazu gehören Änderungen an der Prozessstufe Auswahl, die Klarstellung der Anerkennung von bestehenden Zertifikaten, Ergänzung von Richtlinien zur Auditierung von Multi-Standorten, Überarbeitung von Ermittlungsmethoden, Überarbeitung der Bewertung von Nichtkonformitäten und Ergänzen von Anforderungen zur Festlegung der Ermittlungszeit. So haben die Pilotierungen bspw. gezeigt, dass eine umfassende Vorbereitung durch den Cloud-Anbieter notwendig ist, damit das Zertifizierungsverfahren und insb. die Ermittlungstätigkeiten durch die Zertifizierungsstelle effizient und wirtschaftlich tragbar durchgeführt werden können. Der Cloud-Anbieter sollte bereits vor Beginn der Zertifizierung umfassende Dokumentationen bereitstellen, damit u.a. der Zertifizierungsgegenstand festgelegt, der Ermittlungsumfang (Scope) abgegrenzt und bereits eine Vorprüfung der Erfüllung von Kriterien durchgeführt werden können.

Am 04.02.2020 wurde das KBP und allen weiteren Unterlagen zur Prüfung auf Akkreditierungsfähigkeit bei der DAkkS eingereicht. Die DAkkS hat am 11.08.2020 die Ergebnisse der Prüfung bekannt geben, bei der neun Abweichungen zu den Normen und Anforderungen der DAkkS identifiziert wurden. Das AUDITOR-Konsortium hat daraufhin Änderungen am KBP, den Ermittlungsmethoden, dem Modularitätskonzept sowie weiteren Begleitdokumenten (bspw. Musterzertifikate) vorgenommen und diese zur erneuten Prüfung bei der DAkkS eingereicht. Die DAkkS hat die Änderungen angenommen und aus ihrer Sicht die Prüfung erfolgreich abschließen können. Im Rahmen der nationalen Prüfung durch die Datenschutz-Aufsichtsbehörde von NRW wurden kleinere Änderungen am KBP durchgeführt. Das KBP ist formal seit dem 10.09.2024 bei der DAkkS als akkreditierungsfähiges Zertifizierungsprogramm gelistet.

1.4. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Das Projekt AUDITOR baute durch die interdisziplinäre Expertise des Konsortiums auf bestehende Normen, dem Stand der Technik, aktuellen wissenschaftlichen Entwicklungen inklusive eigener Veröffentlichungen und der Erfahrungen aus vorrangegangen Projekte auf.

Zur möglichst praxisnahen Entwicklung wurden die einschlägigen internationalen Normen bzw. Standards und hoch relevanten (nationalen) Cloud-Dienst-Zertifizierungen berücksichtigt. Hierzu zählen

bspw. Standards aus der ISO/IEC-27000-Reihe (beispielsweise ISO/IEC 27018) und relevante Kriterienwerke (zum Beispiel C5 und ESCloud). Bei der technischen Umsetzung wurden verschiedene Umsetzungsmöglichkeiten rechtlicher Anforderungen durch den Verweis auf Standards (zum Beispiel einschlägige ISO-Standards und nationale Regularien) und einschlägige Kriterienwerke (zum Beispiel TCDP und C5) in Betracht gezogen. Des Weiteren wurde durch das Modularisierungskonzept eine Grundlage geschaffen bestehende Zertifizierungen anzuerkennen (siehe Kapitel 2.1.4).

Zur Zertifizierung von Cloud-Diensten existierten zu Beginn des AUDITOR Projektes einige punktuelle, größtenteils bereits abgeschlossene Projekte, von denen allerdings keins die Forschungsfragen des AUDITOR-Projekts adressiert. Dennoch wurden diese Projekte hinsichtlich ihrer Projektergebnisse und der Verwendbarkeit dieser analysiert. Zu nennen sind beispielsweise das Projekt „Next Generation Certification“ (NGCert), gefördert durch das Bundesministerium für Bildung und Forschung (BMBF), das dynamische Zertifizierungen untersucht, das heißt die teilautomatisierte Überprüfung einzelner Zertifizierungsaspekte und deren Einbindung in ein dynamisches Zertifizierungsverfahren. Das Projekt NGCert endete am 31. Dezember 2017. Zu nennen ist daneben VeriMetrix, ebenfalls vom BMBF gefördert, das bereits zum 30. Juni 2016 auslief und das sich mit der Definition und Verifikation von Kennzahlen für den Datenschutz in Cloud-Anwendungen beschäftigt hat.

Das Konsortium brachte komplementäre Vorarbeiten und umfangreiche Erfahrungen rund um Zertifizierungen von Cloud-Diensten in das Projekt mit ein. Das Karlsruher Institut für Technologie (KIT) hat im Rahmen der Forschungsprojekte „Value4Cloud“ und „NGCert“ Grundlagen zum Verständnis der Rolle von Cloud-Dienst-Zertifizierungen erarbeitet und realweltlich in Zusammenarbeit mit der Industrie und Wirtschaft erprobt. Dabei stellen insbesondere eine entwickelte Taxonomie für Kriterien einer Cloud-Dienst-Zertifizierung sowie ein entwickelter Kriterienkatalog für die Zertifizierung von Cloud-Diensten für dieses Vorhaben relevante Arbeitsergebnisse dar. Das Fachgebiet Rechtswissenschaft an der Universität Kassel hat in einem Gutachten für das Bundesministerium für Forschung und Technologie 1995/96 erstmals ein Datenschutzaudit vorgeschlagen, und im Jahr 1999 ein umfangreiches Konzept für eine Datenschutzaudit entworfen und in dem Gutachten „Modernisierung des Datenschutzrechts“ für das Bundesministerium des Innern (BMI) konkretisiert. Die Universität Kassel kann auf umfangreiche weitere Vorarbeiten im Trusted Cloud Programm verweisen und war am Projekt „Sealed Cloud“ beteiligt. Ferner wurden in den Forschungsprojekten „Cloud Computing – Technik, Sicherheit und rechtliche Gestaltung“ und „Value4Cloud“ Rechtsfragen des Cloud Computing bearbeitet. Zudem wurden zahlreiche Vorarbeiten zur Datenschutz-Grundverordnung und Fragen der Weiterentwicklung des Datenschutzrechts geleistet. Ferner brachten CLOUD&HEAT, ecsec und Hornetsecurity technische Expertise bei der Bereitstellung von Cloud-Diensten sowie Erfahrungen bei der Durchführung von Forschungsprojekten mit. Die datenschutz cert und eco e.V. unterstützten das Vorhaben durch ihre Erfahrung und ihr Wissen über Datenschutz- und Cloud-Dienst-Zertifizierungen und die methodischen Anforderungen zur Erarbeitung von Prüfkriterien. Das DIN konnte ihre Erfahrung bei der Erarbeitung von Normen und Spezifikationen für Wirtschaft, Staat und Gesellschaft einbringen.

1.5. Zusammenarbeit mit anderen Stellen

Das AUDITOR Projekt war aufgrund der interdisziplinären Ausrichtung der einzelnen Konsortialpartner durch eine enge und kontinuierliche Zusammenarbeit geprägt. Die Zusammenarbeit hatte neben den juristischen und technischen Fragestellungen die Gewährleistung der Praxistauglichkeit der zu entwickelnden Zertifizierung insb. für KMUs zum Ziel. Dies wurde durch ein stetig wachsendes Netzwerk von assoziierten Partnern (siehe unterhalb) aus unterschiedlichsten Branchen gestärkt. Assoziierte Partner wurden durch gesonderte Kommunikationskanäle, Einladungen zu AUDITOR-Veranstaltungen und teils durch einen direkten Austausch eingebunden und trugen somit ebenfalls zum Projekterfolg bei. Neben den Partnern, die aktiv im operativen Projekt mitgewirkt haben, wurde das AUDITOR Projekt durch einen Expertenbeirat (siehe unterhalb), der in unregelmäßigen Abständen tagte, in ihrer Ausrichtung und strategischen Planung beratend unterstützt.

Assoziierte Partner (Auswahl):

- Der Bundesverband IT-Mittelstand e.V. (BITMi)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- CAS Software AG
- Consultix GmbH
- CRM!ADDON Factory GmbH
- Deutsche Telekom AG
- direkt gruppe GmbH
- ePrivacy GmbH
- Fabasoft Austria GmbH
- Fujitsu Technology Solutions GmbH
- Hornetsecurity GmbH
- IBM Corporation
- 1&1 IONOS Cloud GmbH
- Kompetenznetzwerk Trusted Cloud e.V.
- mediaBEAM GmbH
- Microsoft Deutschland GmbH
- Mitteldeutsche Gesellschaft für Informationssicherheit und Datenschutz mbH
- MKM + PARTNER
- PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
- Propstack GmbH
- Salesforce.com Germany GmbH
- SAP SE
- SCOPE Europe b.v.b.a/s.p.r.l.
- tacticx Consulting GmbH
- TechGDPR DPC GmbH
- TÜV Informationstechnik GmbH
- TÜV Rheinland AG
- TÜV SÜD Management Service GmbH
- Uniscon GmbH
- VIVAI Software AG, Smart Service Power
- VOICE-Bundesverband der IT-Anwender e. V.
- WALLSEC GmbH
- x-ion GmbH

Expertenbeirat:

- Susanne Dehmel, Bitkom e.V.
- Dr. Thilo Weichert, Netzwerk Datenschutzexpertise
- Prof. Dr. Helmut Krcmar, Technische Universität München
- Prof. Dr. Georg Borges, Universität des Saarlandes
- LL.M. Frederick Richter, Stiftung Datenschutz

Neben der projektinternen Zusammenarbeit gab es auch zahlreiche Zusammenarbeiten, die bspw. im Rahmen des Bewilligungsprozesses stattgefunden haben. Hierbei sind insbesondere die DAkkS und die Datenschutz-Aufsichtsbehörde von NRW hervorzuheben. Primär ging es bei dieser Zusammenarbeit nicht um die aktive Gestaltung der Projektergebnisse, sondern um Feedback und rechtliche Vorgaben, die vom Konsortium umgesetzt werden mussten.

Das KIT organisierte zudem gemeinsam mit der Universität Kassel, TrustedCloud und dem BMWK den Lenkungsausschuss von AUDITOR. Dieser tagte in unregelmäßigen Zeitabständen und sorgte für die politische und inhaltliche Abstimmung von AUDITOR. Salesforce und die Deutsche Telekom haben zudem eine „Go-To-Market“-Arbeitsgruppe initiiert, um gemeinsam mit dem BMWK und dem Konsortium die Anwendbarkeit von AUDITOR durch geeignete Maßnahmen zu flankieren.

Im Rahmen von diversen Workshops, Messeauftritten und ähnlichen Veranstaltungen wurden neben den bereits aufgeführten Stellen auch die breite Öffentlichkeit eingebunden. Die Veranstaltungen hatten in der Regel nicht nur einen informierenden Charakter, sondern förderten den regen Austausch, sodass die generierten Impulse und Ideen aus diesen Veranstaltungen in die Projektergebnisse von AUDITOR aktiv eingeflossen sind. Eine Übersicht dieser Veranstaltungen ist in Kapitel 2.6.4 aufgeführt.

2. Eingehende Darstellung des Projektes

2.1. Erzielte Ergebnisse im Einzelnen

Das AUDITOR-Projekt hat die erste Datenschutzzertifizierung für Cloud-Dienste in Europa erfolgreich entwickelt und bewilligen lassen. Kernbestandteil dieser Zertifizierung sind insbesondere der Zertifizierungsgegenstand, der Kriterienkatalog, das KBP, Schutzklassen- und Modularisierungskonzepte, die Erprobung und Standardisierung des Verfahrens sowie dessen Bewilligung (Tabelle 1). Die Folgenden Kapitel skizzieren die Arbeiten und Ergebnisse entsprechend.

Tabelle 1. Übersicht der zentralen Arbeitsergebnisse sowie deren Arbeitspakete

Meilenstein / Ergebnis	**Arbeitspakete**	
	Initialer Antrag	Folgeantrag
Zertifizierungsgegenstand	Indirekt AP1	-
Kriterienkatalog	AP 1	AP 2
Konformitätsbewertungsprogramm	AP 2	AP 3
Schutzklassen- und Modularisierungskonzepte	AP 4	-
Lessons Learned aus den Pilotierungen	AP 7	AP 4
DIN SPEC	AP 3	AP 5
Bewilligung des Zertifizierungsverfahrens	Indirekt AP 1, AP 2, AP 5, AP 9	AP 1

2.1.1. Zertifizierungsgegenstand

Aufgabenbereich:	Kriterienkatalog und Zertifizierungsverfahren
Leitung:	Universität Kassel
Arbeitspakete gemäß GVB	(Indirekt) AP 1
Korrespondierende Teilziele	TZ1 Kriterienkatalog, TZ2 Zertifizierungsverfahren
Wesentliche Ergebnisse	• Spezifikation des AUDITOR-Zertifizierungsgegenstandes

Zur Durchführung des AUDITOR-Zertifizierungsverfahrens musste zunächst der Zertifizierungsgegenstand definiert werden. Der Zertifizierungsgegenstand beschreibt das im Rahmen von AUDITOR zu überprüfende Untersuchungsobjekt auf Basis der Zertifizierungskriterien des AUDITOR-Kriterienkatalogs. Die Festlegung stellte sich zu Projektbeginn als besonders schwierig heraus, da kontroverse juristische Meinungen vorherrschten. Eine klare Umgrenzung des Zertifizierungsgegenstandes ist wichtig, da dieser die Grundlage für die spätere Aussage des Zertifikats regelt. Denn sowohl die Cloud-Anbieter (d.h. die Zertifizierten) als auch die Cloud-Nutzer als Kunden des zertifizierten Cloud-Dienstes müssen sich auf den Aussagegehalt verlassen können. Schließlich wollen die Cloud-Anbieter mit der Zertifizierung eine tatsächlich zutreffende Verordnungs- und

Datenschutzkonformität nachweisen und am Markt gemäß den Lauterkeitsregeln mit dieser werben. Der Cloud-Nutzer möchte durch die Zertifizierung darauf vertrauen können, dass der verwendete Cloud-Dienst datenschutzkonform ist, um somit seine Haftungsrisiken gegenüber Endverbrauchern möglichst gering zu halten.

Den Zertifizierungsgegenstand des AUDITOR-Verfahrens bilden Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud-Diensten. Eine Datenverarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Den Zertifizierungsgegenstand bilden Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Schwerpunktmäßig werden im AUDITOR-Verfahren die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Es werden aber auch Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können und damit er rechtliche Pflichten erfüllen kann.

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die Cloud-Anbieter als Adressaten des AUDITOR-Zertifizierungsverfahrens beachten müssen: 1. personenbezogene Daten, 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die zu Datenschutzkonzepten und -managementsystemen zusammengefasst sind. Der gesamte Datenverarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Kritische Datenverarbeitungsvorgänge dürfen nicht ausgeklammert werden, um ein ‚Rosinenpicken' zu verhindern.

Die Zertifizierung richtet sich im Allgemeinen an Cloud-Anbieter, unabhängig vom jeweiligen Dienstmodell, wie bspw. Software-as-a Service, Platform-as-a-Service und Infrastructure-as-a-Service. Dadurch kann AUDITOR für alle am Markt befindlichen Cloud-Diensten angewendet werden. Schwerpunkt der Zertifizierung sind Datenverarbeitungsvorgänge des Cloud-Anbieters in seiner Rolle

als Auftragsverarbeiter. Daneben verarbeitet der Cloud-Anbieter jedoch immer auch personenbezogene Daten der Cloud-Kunden, um diesem den gewünschten Cloud-Dienst bereitstellen zu können. Hierzu zählen Bestandsdaten des Cloud-Kunden (bspw. Namen, Adressen, Zahlungsdaten) sowie Nutzungsdaten (bspw. Benutzername, IP-Adressen, Log-Daten). Bei dieser Datenverarbeitung entscheidet er über die Zwecke und Mittel der Verarbeitung und ist daher Verantwortlicher (gemäß Art. 4 Nr. 7 DSGVO). Diese Datenverarbeitung ist erforderlich zur Diensterbringung und muss daher ebenfalls zwingend geprüft werden. Die AUDITOR-Zertifizierung stellt damit sicher, dass Cloud-Kunden ganzheitlich geschützt werden, im Gegensatz zu anderen Zertifizierungen am Markt, welche ausschließlich die Auftragsverarbeitung zertifizieren.

Eine umfassende Herleitung und Definition des Zertifizierungsgegenstandes kann im Ergebnisdokument *„Zertifizierungsgegenstand“* nachgelesen werden.

2.1.2. Kriterienkatalog

Aufgabenbereich:	Kriterienkatalog
Leitung:	Universität Kassel
Arbeitspakete gemäß GVB	• AP 1 • AP 2 Folgeantrag
Korrespondierende Teilziele	TZ1 Kriterienkatalog
Wesentliche Ergebnisse	• AUDITOR-Kriterienkatalog • Umsetzungshinweise • Hinweise für Nachweise im Rahmen des Zertifizierungsverfahrens • Kriterien-Mapping-Tabellen zu bestehenden Zertifizierungen • Vorbereitung der Europäisierung des Zertifizierungsverfahrens

Ein wesentliches Ziel des Projektes bestand in der Entwicklung eines Kriterienkatalogs, welcher der Datenschutzzertifizierung zugrunde liegt. Der AUDITOR-Kriterienkatalog überführt die technikneutralen Vorschriften der Datenschutz-Grundverordnung an die Auftragsverarbeitung in prüffähige, normative Kriterien, die ein Cloud-Anbieter erfüllen muss, wenn er seine Datenverarbeitungsvorgänge zertifizieren lassen möchte. Hierbei wurden insbesondere aus den Vorgaben der Datenschutz-Grundverordnung und den einschlägigen Normen im Bereich Datenschutz, Datensicherheit und Privatsphäre Zertifizierungskriterien abgeleitet, klassifiziert und damit ein umfassender Zertifizierungskriterienkatalog entwickelt. Der Katalog umfasst alle relevanten Bereiche, wie Kriterien zur IT-Sicherheit (z.B. Zugriffs- und Zugangssicherheit) sowie neue Anforderungen der Datenschutz-Grundverordnung (z.B. Wahrung von Betroffenenrechten) und zum Schutz der Privatsphäre (z.B. Privacy by Design & Default).

Zur Ableitung der Kriterien wurde die Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen (KORA) angewendet. Die Methode KORA bietet eine regelbasierte Vorgehensweise zur Überführung abstrakter rechtlicher Vorgaben in konkrete technische Gestaltungsvorschläge. Sie grenzt sich von anderen Vorgehensweisen vor allem dadurch ab, dass sie neben dem einfachen Gesetz auch und gerade verfassungsrechtliche Vorgaben berücksichtigt, um eine bestmögliche Verwirklichung von Grundrechten durch die zu entwickelnde Technik zu erreichen. KORA

erreicht dies in einem vierstufigen Begründungs- und Übersetzungsprozess. In einem ersten Schritt wurden aus gesetzlichen Vorgaben insbesondere der Datenschutz-Grundverordnung funktionsbezogene rechtliche Anforderungen, in einem zweiten Schritt aus diesen techniknahe rechtliche Kriterien konkretisiert. Aus diesen wurden in einem dritten Schritt technische Gestaltungsziele und in einem vierten Schritt technische Gestaltungsvorschläge abgeleitet.

Neben den Kriterien umfasst der Katalog auch Erläuterungen, umfassende Umsetzungshinweise und Vorschläge zum Nachweis der Konformität während des Zertifizierungsverfahrens (Abbildung 3). Die Erläuterungen sollen das Verständnis der Kriterien und ihre Herleitung aus der Datenschutz-Grundverordnung erleichtern. Umsetzungshinweise sind exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien, die jedoch keinen verpflichtenden Charakter haben. Auch sind Umsetzungshinweise nicht abschließend, sondern beschreiben zentrale Umsetzungen für die Kriterien. Die Umsetzungshinweise orientieren sich dabei, wo es angemessen ist, an bestehenden Industriestandards, Normen und Best-Practices. So wird bspw. insbesondere bei den Kriterien zur Gewährleistung der Datensicherheit auf die ISO/IEC 27001/2 und das BSI C5 verwiesen. Ergänzende Kriterien-Mapping-Tabellen zu bestehenden Zertifizierungen wurden angefertigt. Zudem finden sich zu jedem Kriterium „Nachweise“, die eine Antwort auf die Frage liefern, wie das Vorliegen der Kriterien im konkreten Zertifizierungsverfahren erwiesen werden kann. Sie stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Dabei wird bspw. die Vorlage von Dokumentationen zur Prüfung durch die Zertifizierungsstelle vorgeschlagen, oder die Durchführung einer Vor-Ort-Auditierung durch die Zertifizierungsstelle als Nachweis zur Umsetzung von dokumentierten Maßnahmen vorausgesetzt. Es besteht keine Verpflichtung, die Nachweise gemäß diesem Dokument zu erbringen. Mit seinen vier Bestandteilen stellt der Katalog somit umfassende Hilfestellungen für Cloud-Anbieter bereit und schafft Transparenz über den Umfang der Zertifizierung bei Cloud-Kunden.

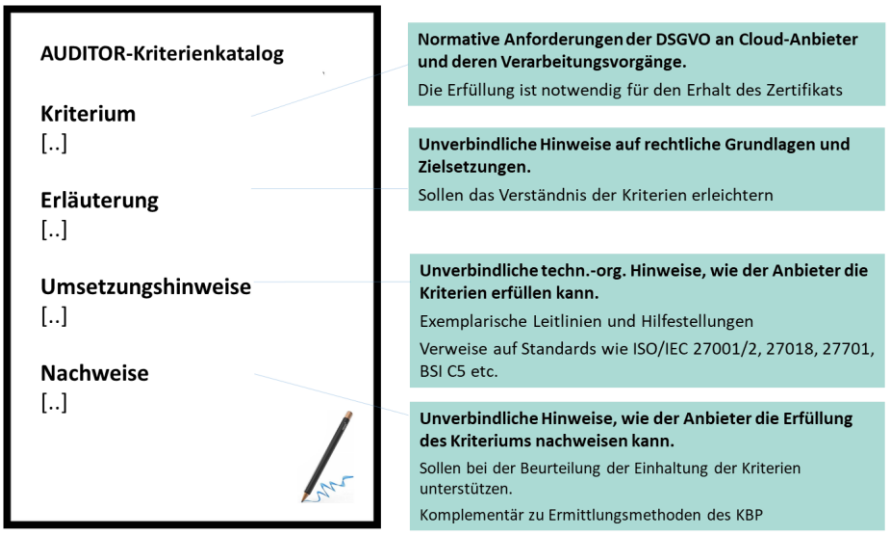

Abbildung 3. Schematische Darstellung des AUDITOR-Kriterienkatalogs.

Die Kriterien sind in thematisch zusammenhängende Kapitel gegliedert. Insgesamt beinhaltet der Kriterienkatalog sieben Kapitel, welche im Folgenden zusammengefasst werden.

Kapitel I enthält Kriterien, die die rechtsverbindliche Vereinbarung des Cloud-Anbieters mit dem Cloud-Nutzer über die Auftragsverarbeitung betreffen. Die Kriterien bilden die einzelnen gesetzlichen Anforderungen von Art. 28 Abs. 3 DSGVO ab, beispielsweise hinsichtlich der Bestimmung von Gegenstand und Dauer der Verarbeitung, der Festlegung der Weisungsbefugnisse des Cloud-Nutzers gegenüber dem Cloud-Anbieter oder der Verantwortung des Cloud-Anbieters die mit der Datenverarbeitung betrauten Mitarbeiter zur Vertraulichkeit zu verpflichten.

Hoher Stellenwert kommt auch den Kriterien des Kapitels II zu den Rechten und Pflichten des Cloud-Anbieters zu. So sind beispielsweise Kriterien formuliert worden, um die rechtlichen Anforderungen zur Datensicherheit aus Art. 32 DSGVO cloud-spezifisch zu konkretisieren. Da der Cloud-Anbieter technische und organisatorische Maßnahmen in Abhängigkeit vom Risiko der ausgelagerten Datenverarbeitung treffen muss, werden die Kriterien zur Datensicherheit in drei Schutzklassen spezifiziert (siehe Kapitel 2.1.4). Die Umsetzungshinweise zu den Kriterien der Datensicherheit verweisen, soweit es zweckmäßig ist, auf anerkannte ISO-Normen wie die der Normenreihe ISO/IEC 27000, die in erster Linie der Gewährleistung von IT-Sicherheit dienen. IT-Sicherheit und Datensicherheit weisen grundsätzlich unterschiedliche Zielrichtungen auf. Jedoch adressiert Art. 32 Abs. 1 DSGVO mit Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit klassische IT-Sicherheitsziele, sodass dieselben technischen und organisatorischen Maßnahmen häufig sowohl der Gewährleistung von IT-Sicherheit und Datensicherheit dienen. Verfügt der Cloud-Anbieter daher über eine IT-Sicherheitszertifizierung nach internationalen Standards, kann diese auch im Rahmen der AUDITOR-Zertifizierung herangezogen und bei der Prüfung anerkannt werden (siehe Kapitel 2.1.4).

Kapitel III des Kriterienkatalogs behandelt das Datenschutzmanagementsystem des Cloud-Anbieters. Das Kapitel enthält beispielsweise Kriterien für die Benennung eines Datenschutzbeauftragten 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, für die Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 2 DSGVO und für die Errichtung eines Kontrollsystems nach Art. 24 DSGVO, das sicherstellen soll, dass die Umsetzung der Kriterien des Kriterienkatalogs regelmäßig intern durch den Cloud-Anbieter geprüft wird.

Weitere Kapitel des Kriterienkatalogs verpflichten den Cloud-Anbieter zu Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen (Kapitel IV), zur Gewährleistung eines gleichbleibenden Datenschutzniveaus trotz des Einsatzes weiterer Auftragsverarbeiter im Rahmen von Subauftragsverarbeitungen (Kapitel V) und zum Nachweis geeigneter Garantien für die Datenübermittlung, wenn die Auftragsverarbeitung außerhalb der EU und des Europäischer Wirtschaftsraums stattfinden soll (Kapitel VI). Das letzte Kapitel enthält die Kriterien an den Cloud-Anbieter als Verantwortlichen für die Datenverarbeitung, die zur Durchführung des Auftrags mit dem Cloud-Nutzer für die Erbringung, Nutzung und Abrechnung des Cloud-Dienstes erforderlich ist.

Im Zuge der Weiterentwicklung zu einem europäischen Gütesiegel wurden national-spezifische Anhänge mit weiteren Kriterien angefügt, welche nur in bestimmten EU-Mitgliedstaaten relevant sind, da nationale Spezifika diese erfordern. So sind bspw. länderspezifische Anhänge für Bulgarien, Dänemark, Belgien, und der Slowakei angefertigt worden, um ergänzende oder verfeinerte AUDITOR-Kriterien aufzunehmen.

Der Kriterienkatalog ist öffentlich verfügbar. Eine umfassende Beschreibung und alle Kriterien können im Ergebnisdokument „*Kriterienkatalog*“ nachgelesen werden.

2.1.3. Konformitätsbewertungsprogramm

Aufgabenbereich:	Zertifizierungsverfahren
Leitung:	Karlsruher Institut für Technologie
Arbeitspakete gemäß GVB	• AP 2 • AP 3 Folgeantrag
Korrespondierende Teilziele	TZ2 Zertifizierungsverfahren
Wesentliche Ergebnisse	• AUDITOR-KBP • Ermittlungsmethoden • Muster für Zertifikat und Gütesiegel

Gemäß Art. 43 Abs. 1 Satz 1 DSGVO können Zertifizierungsstellen neben Aufsichtsbehörden Zertifizierungen erteilen. Eine Zertifizierungsstelle darf ihre Tätigkeit jedoch nur aufnehmen, wenn sie durch die DAkkS in Zusammenarbeit mit der zuständigen Aufsichtsbehörde akkreditiert wurde. Voraussetzung der Akkreditierung ist die Einhaltung der Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. ISO/IEC 17065. Maßgeblich für die Akkreditierung ist das KBP, welches als Regelwerk sicherstellt, dass die mit der Zertifizierung verbundene Aussage auf wissenschaftlich rückführbare und systematische Weise getroffen wurde. Die Akkreditierung von Zertifizierungsstellen schafft Vertrauen und eine Vergleichbarkeit zwischen Zertifizierungsverfahren.

Neben dem Kriterienkatalog wurde daher ein KBP entworfen, welches die Anforderungen an Zertifizierungsstellen und Regelwerke zur Durchführung der Zertifizierung festlegt. Hierzu zählen geeignete Organisationsstrukturen, Ermittlungsmethoden und Verfahren zur Vergabe und zur Durchführung einer anerkannten Datenschutzzertifizierung. Bei der Spezifikation wurde insb. auch auf die Modularität des Verfahrens geachtet, um die Bedürfnisse von KMU und die Vielfalt der Cloud-Dienste berücksichtigen zu können. Das Modularisierungskonzept regelt unter anderem die Anerkennung bestehender Zertifizierungen (z.B. Sicherheitsmanagement ISO/IEC 27001) oder zukünftiger IT-Sicherheitszertifikate (gemäß EU Cybersecurity Act), um doppelte Prüfungen zu vermeiden und somit Kosten zu reduzieren.

Das AUDITOR-KBP beschreibt die von der Zertifizierungsstelle zu erfüllenden Grundsätze und umfasst im Wesentlichen Anforderungen an die Zertifizierungsstelle und den Zertifizierungsprozess. Die wesentlichen Inhalte des KBPs werden im Folgenden zusammengefasst.

Um Vertrauen in ihre Tätigkeiten und ihre Ergebnisse zu schaffen, ist es für die Zertifizierungsstellen und ihr Personal erforderlich, unparteiisch zu sein und als unparteiisch empfunden zu werden. Dabei beschreibt Unparteilichkeit das Vorhandensein von Unabhängigkeit und Objektivität. Um Interessenkonflikte zu verhindern, darf eine Zertifizierungsstelle bspw. keine Beratungsdienstleistungen im Vorfeld bei einem zu zertifizierenden Cloud-Anbieter durchgeführt haben.

Weitere Anforderungen an die Zertifizierungsstelle betreffen unter anderem die Struktur und Ressourcen der Zertifizierungsstelle und die Etablierung und den Betrieb eines Managementsystems. Von hoher Bedeutung sind hierbei Anforderungen an personelle Kompetenzen der Zertifizierungsstelle. Es werden umfassende Fachkompetenzen in technischer und juristischer Hinsicht gefordert, wie bspw. Kenntnisse der relevanten Normen zur Konformitätsbewertung (insbesondere ISO-Normen und einschlägige Fachgesetze), Kenntnisse im Datenschutzrecht (DSGVO/ BDSG) sowie Kenntnisse über technische Grundlagen von Datenverarbeitungsvorgängen von Cloud-Diensten.

Weiterhin enthält das KBP Richtlinien für die Durchführung der sechs Prozessphasen eines Zertifizierungsverfahrens: Auswahl, Ermittlung, Bewertung, Entscheidung, Bestätigung und Überwachung. Bei der Auswahl wird zunächst der Zertifizierungsgegenstand dargestellt und abgegrenzt und eine Zertifizierungsvereinbarung abgestimmt. Zudem werden planende und vorbereitende Tätigkeiten definiert, damit für die nachfolgende Ermittlung alle erforderlichen Informationen zur Verfügung stehen. Bei der Ermittlung werden im KBP Prüfmethoden (sog. Ermittlungsmethoden) spezifiziert, anhand derer festgestellt werden soll, ob die Datenverarbeitungsvorgänge die im Kriterienkatalog festgelegten Zertifizierungskriterien erfüllen. Hierzu zählen bspw. technische Tests, Inspektionen, Dokumentenprüfungen und Vor-Ort-Auditierungen. Im Rahmen der Bewertung verifiziert die Zertifizierungsstelle, ob die Auswahl- und Ermittlungstätigkeiten und deren Ergebnisse hinsichtlich der Erfüllung der festgelegten Zertifizierungskriterien durch die Datenverarbeitungsvorgänge geeignet, angemessen und wirksam sind, und entscheidet anschließend über die Vergabe des Zertifikats. Dabei hat die Zertifizierungsstelle die zuständige Datenschutz-Aufsichtsbehörde über die Zertifizierung schriftlich mindestens eine Woche vor Erteilung der Zertifizierung zu unterrichten. Nach Genehmigung durch die Aufsichtsbehörde kann das Zertifikat erteilt werden. Im Rahmen des Projektes wurden Muster-Zertifikate und -Gütesiegel erstellt, welche die wesentlichen Inhalte darstellen.

Darüber hinaus legt das KBP auch Anforderungen an die Überwachung fest. Die Überwachung umfasst systematische, sich wiederholende Konformitätsbewertungstätigkeiten, um zu prüfen, ob die Gültigkeit des Zertifikats aufrechterhalten werden kann. Dafür müssen die Datenverarbeitungsvorgänge während der Gültigkeitsdauer des Zertifikats mindestens einer jährlichen Zwischenprüfung unterzogen werden. Darüber hinaus können anlassbezogene Überwachungen erfolgen, wenn Auffälligkeiten bestehen und zu befürchten ist, dass Zertifizierungsanforderungen nicht eingehalten werden.

Bei der Spezifikation eines KBP ist die Festlegung der Prüfung der einzelnen Kriterien wesentlich, um sicherzustellen, dass verschiedene Prüfer zum gleichen Ergebnis der Konformitätsbewertung kommen. Das AUDITOR-KBP umfasst die Prüfung der vom Cloud-Anbieter zur Verfügung gestellten Dokumentationen, Inspektionen (im Sinne der ISO/IEC 17020), Prüfungen (im Sinne der ISO/IEC

17025:2017), Audits (im Sinne der ISO/IEC 17021-1:2015), und Entwicklungs- und Designprüfungen. Die Prüfungen können sich auf unterschiedliche Ermittlungsobjekte beziehen, darunter Verträge, Prozesse, Diensteigenschaften, Infrastruktur- und Softwarekomponenten und Mitarbeiter des Cloud-Anbieters. Für jedes Kriterium gibt das AUDITOR-KBP individuelle Vorgaben zur Durchführung der Prüfung an. Um bspw. die Ernennung eines Datenschutzbeauftragen nachzuweisen, sollten interne und externe Dokumente geprüft werden. Geeignete Dokumente zum Nachweis der tatsächlichen Ernennung können bspw. die Datenschutzerklärung oder das Verzeichnis von Verarbeitungstätigkeiten mit der entsprechenden Angabe oder Tätigkeitsbeschreibungen in Arbeitsverträgen sein. Zur Überprüfung der fachlichen Qualifikation des Datenschutzbeauftragen hat der Cloud-Anbieter Dokumente wie bspw. Zeugnisse, Lebensläufe oder Teilnahmebescheinigungen über relevante Weiterbildungen vorzulegen, aus denen hervorgeht, dass der Datenschutzbeauftrage das erforderliche Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis verfügt. Informationen zur Prüfung der jeweiligen Kriterien wurden in den Ermittlungsmethoden festgehalten.

Das AUDITOR-KBP ist zur Wahrung von Wettbewerbsvorteilen nicht öffentlich einsehbar, kann aber beim Programmeigner Kompetenznetzwerk Trusted Cloud e.V. angefragt werden. Eine Kurzfassung wurde öffentlich freigegeben.

2.1.4. Modularisierung: Schutzklassen- und Modularisierungskonzept

Aufgabenbereich:	Zertifizierungsverfahren
Leitung:	Universität Kassel und Karlsruher Institut für Technologie
Arbeitspakete gemäß GVB	• AP 4
Korrespondierende Teilziele	TZ1 Kriterienkatalog, TZ2 Zertifizierungsverfahren
Wesentliche Ergebnisse	• Schutzklassenkonzept • Modularitätskonzept

Aufbauend auf dem TCDP wurde auch für AUDITOR eine Modularisierung angestrebt. Ziel der Modularisierung ist es, das Zertifizierungsverfahren möglichst passend für den jeweiligen Datenverarbeitungsgang zu gestalten und Aufwände für die Zertifizierung zu reduzieren. Dazu wurden zwei maßgebliche Dokumente erstellt: das Schutzklassen- und das Modularitätskonzept.

Der Kriterienkatalog nimmt bei einigen Kriterien eine Unterscheidung nach Schutzklassen vor und legt für diese unterschiedliche Anforderungen fest, die erfüllt werden müssen. Schutzklassen stellen bei der Datenschutzzertifizierung ein wichtiges Instrument dar, da mit ihnen der individuelle Schutzbedarf von Datenverarbeitungsvorgängen und dessen Erfüllung durch zertifizierte Cloud-Dienste ausgedrückt werden kann. So sind beispielsweise Kriterien formuliert worden, um die rechtlichen Anforderungen zur Datensicherheit aus Art. 32 DSGVO cloud-spezifisch zu konkretisieren. Da der Cloud-Anbieter technische und organisatorische Maßnahmen in Abhängigkeit vom Risiko der ausgelagerten Datenverarbeitung treffen muss, werden die Kriterien zur Datensicherheit in drei Schutzklassen spezifiziert. Je nachdem wie schutzbedürftig die in die Cloud ausgelagerten Daten aufgrund ihrer Art

und den Umständen ihrer Verarbeitung sind, muss der Cloud-Anbieter normale, hohe oder sehr hohe Schutzanforderungen in Form von technischen und organisatorischen Maßnahmen implementieren. So ist die Verarbeitung medizinischer Patientendaten durch Maßnahmen der höchsten Schutzklasse abzusichern. Beispielweise fordert der Kriterienkatalog für die höchste Schutzklasse, dass Manipulationen von Protokollierungsinstanzen und -dateien hinreichend sicher ausgeschlossen werden. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Manipulationen ein. Jede Manipulation und möglichst auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können. Die Differenzierung in Schutzklassen gewährleistet, dass Cloud-Anbieter Schutzmaßnahmen implementieren, die dem Schutzbedarf der jeweiligen Datenverarbeitungen angemessen sind. Auf diese Weise verhindern Schutzklassen unangemessen hohe Kosten, aber auch unzureichende Schutzmaßnahmen.

Eine umfassende Beschreibung und Festlegung der Schutzklassen kann im Ergebnisdokument *„Schutzklassenkonzept“* nachgelesen werden.

Ein weiteres Ziel des Projektes war die Erarbeitung eines Modularisierungskonzepts für die Zertifizierung. Durch eine modulare Zertifizierung wird die erneute Prüfung von Anforderungen, die bereits nach AUDITOR zertifiziert sind, entbehrlich. Ziel einer modularen Zertifizierung sollte sein, dass ein Cloud-Dienst und dessen Bestandteile (Module) nicht erneut überprüft werden müssen, wenn es um die Zertifizierung von darauf aufbauenden Bestandteilen geht.

Das AUDITOR-Modularisierungskonzept beschreibt die Modularisierung von Datenverarbeitungsvorgängen. Durch das AUDITOR-Modularisierungskonzept wird die Flexibilität bei der Zertifizierung erhöht. So ist es beispielsweise möglich, dass ein Cloud-Dienst vollumfänglich oder lediglich ein einzelner Datenverarbeitungsvorgang des Cloud-Dienstes zertifiziert wird. Die modulare Zertifizierung spiegelt den Umstand wider, dass Datenverarbeitungsvorgänge häufig modular aufgebaut sind. So kann ein Cloud-Anbieter, der mehrere Cloud-Dienste anbietet, die Zertifizierung dieser anhand der Zusammenhänge untereinander kombinieren bzw. vereinfachen. Die Modularisierung beschreibt einen Vorgang, bei dem ein Cloud-Dienst und die entsprechenden Datenverarbeitungsvorgänge in einzelne Module aufgeteilt werden. So ist es möglich, dass ein Cloud-Dienst vollumfänglich zertifiziert wird, indem alle relevanten Datenverarbeitungsvorgänge gemeinsam zertifiziert werden. Dabei entspricht der Cloud-Dienst dann einem Modul. Darüber hinaus ist es auch möglich, lediglich einen einzelnen Datenverarbeitungsvorgang des Cloud-Dienstes zu zertifizieren. Dabei ist der Datenverarbeitungsvorgang dann als einzelnes Modul zu verstehen. Bereits zertifizierte Module können dann in zukünftigen Zertifizierungsverfahren anerkannt werden, sodass der Aufwand und die Kosten für zukünftige Zertifizierungen verringert werden. Trotz der Modularisierung muss sichergestellt sein, dass die modularen Datenverarbeitungsvorgänge eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen und keine kritischen Verarbeitungsvorgänge ausgeklammert werden.

Die Modularisierung der Zertifizierung kann sowohl auf horizontaler als auch auf vertikaler Ebene erfolgen. In Abbildung 4 wird diese Unterscheidung vereinfacht dargestellt. In der Abbildung bilden die

drei grundlegenden Servicemodelle des Cloud-Computings, also Software-as-a-Service, Platform-as-a-Service und Infrastructure-as-a-Service, die sogenannten Dienst-Ebenen (‚*Cloud-Stack*').

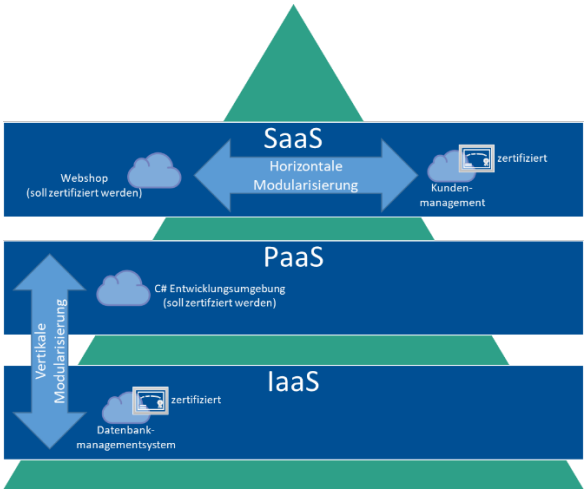

Abbildung 4. Modularisierung der AUDITOR-Zertifizierung.

Darüber hinaus dient das Modularitätskonzept als Grundlage für die Anerkennung von gleichwertigen Zertifizierungen im Rahmen einer AUDITOR-Zertifizierung. Die Anerkennung von bestehenden Zertifikaten wird maßgeblich durch die ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO und der Anforderungen der ISO/IEC 17065 reguliert. Die AUDITOR-Zertifizierung folgt grundsätzlich deren Anforderungen. Daher gibt es nur drei Möglichkeiten im Rahmen des Zertifizierungsprozesses ein anderes Zertifikat als Teilevaluierung anzuerkennen:

(1) Das Zertifikat wurde von einer akkreditierten Zertifizierungsstelle ausgestellt (bspw. ein ISO/IEC 27001 Zertifikat durch eine akkreditierte Zertifizierungsstelle);
(2) Das Zertifikat wurde von einer Stelle ausgestellt, die eine Begutachtung unter Gleichrangigen durchlaufen hat (gem. ISO/IEC 17040:2005);
(3) Das Zertifikat wurde durch eine staatliche Zertifizierungsstelle auf gesetzlicher Grundlage ausgestellt (z.B. EU Cybersecurity Act).

Eine umfassende Erläuterung dieser Fälle kann im Ergebnisdokument „*Modularisierungskonzept*" nachgelesen werden.

2.1.5. Pilotierung

Aufgabenbereich:	Zertifizierungsverfahren
Leitung:	Karlsruher Institut für Technologie und datenschutz cert GmbH
Arbeitspakete gemäß GVB	• AP 7 • AP 4 Folgeantrag
Korrespondierende Teilziele	TZ3 Erprobung
Wesentliche Ergebnisse	• Lessons Learned aus der Erprobung • Überarbeitetes Zertifizierungsverfahren und verbesserter Kriterienkatalog

Das erarbeitete Zertifizierungsverfahren und die im AUDITOR-Projekt erarbeiteten Kriterien wurden schließlich in der Praxis erprobt und validiert. Dabei wurde eine realgetreue Zertifizierung bei kleinen und mittelständischen Cloud-Anbietern durchgeführt, die im Sinne der Ziele der AUDITOR-Zertifizierung typische Kunden der Zertifizierung darstellen. Das wesentliche Ziel der Pilotierung des Zertifizierungsverfahrens war es, das AUDITOR-Zertifizierungsverfahren zu evaluieren und zu validieren. Als zentrale Maßnahme zur Evaluierung und Validierung des AUDITOR-Zertifizierungsverfahrens soll die Durchführung von Pilotzertifizierungen dabei unterstützen, Rückschlüsse über die Anwendbarkeit des Zertifizierungsverfahrens zu erhalten und um konkrete Maßnahmen zu dessen Verbesserung abzuleiten. Die Pilotierungen wurden unter Einhaltung aller Anforderungen des KBP durchgeführt, um eine realweltliche Erprobung sicherzustellen. Die Pilotierungen wurde wissenschaftlich begleitet, sodass die Erkenntnisse zurück in das Projekt geführt werden konnten. Neben der Korrektheit und Anwendbarkeit wurde durch die Forschungseinrichtungen auch die Machbarkeit unter Gesichtspunkten von Wirtschaftlichkeit, Akzeptanz und Marktaussichten untersucht. Dabei hat sich gezeigt, dass AUDITOR einen hohen Reifegrad besitzt und in der Praxis angewendet werden kann.

Im Zeitraum von Juni bis August 2019 wurden drei Pilotzertifizierungen durch die datenschutz cert GmbH in der Rolle der prüfenden Zertifizierungsstelle durchgeführt:

1) Am 17. und 18. Juni 2019 wurde die erste Pilotierung im Rahmen des AUDITOR-Projektes bei der Cloud&Heat GmbH in Frankfurt durch die datenschutz cert GmbH durchgeführt. Unterstützt wurde die Pilotierung durch die Mitteldeutsche Gesellschaft für Informationssicherheit und Datenschutz mbH, das KIT und die Universität Kassel.
2) Am 11. und 12. Juli 2019 wurde die zweite Pilotierung im Rahmen des AUDITOR-Projektes bei der Hornetsecurity GmbH in Hannover durch die datenschutz cert GmbH durchgeführt. Unterstützt wurde die Pilotierung durch das KIT und die Universität Kassel.
3) Zum Abschluss der Pilotierungsphase wurde am 19. und 20. August eine dritte Pilotierung für die ecsec GmbH im Rechenzentrum der noris network AG in Nürnberg durch die datenschutz cert GmbH durchgeführt. Unterstützt wurde die Pilotierung durch das KIT.

Die Pilotierung wurde auf Grundlage des KBP und des Kriterienkatalogs (v0.9) durch die datenschutz cert GmbH durchgeführt, welche bereits langjährige Erfahrungen in der Durchführung von Datenschutzzertifizierungen und weiteren relevanten IT-Sicherheitszertifizierungen (darunter ISO/IEC 27001) vorweisen kann. Wesentliche Aktivitäten im Rahmen der Pilotierung auf Seiten der datenschutz cert GmbH waren:

1. Vorbereitung
    a. Einarbeitung des relevanten Personals der Zertifizierungsstelle in den Kriterienkatalog,
    b. Einarbeitung des relevanten Personals der Zertifizierungsstelle in das KBP,
    c. Verteilung der Aufgaben innerhalb der Zertifizierungsstelle anhand der Anforderungen an das Personal (Kompetenzfeststellungen, Einteilung der Auditteams etc.),

d. Entwicklung eines Vorgehens zur Sammlung relevanter Informationen vom Cloud-Anbieter gemäß des KBP und der AUDITOR-Ermittlungsmethode,
e. Planung und Kalkulation der Aufwände,
f. Planung und Abstimmung mit den Cloud-Anbietern,
g. Prüfung vorgelegter Informationen (Festlegung des Audit-Scopes, soweit möglich, Vorbereitung des Audits etc.),
h. Erarbeitung entsprechender Musterdokumente (Agenda, Auditbericht, Fragebögen, etc.).

2. Vor-Ort Auditierung
    a. Durchführung des Audits anhand bekannter genormter Vorgehensweisen (Audit, Prüfung, Validierung, Verifizierung) des KBP und der AUDITOR-Ermittlungsmethoden,
    b. Arbeit in Auditteams und gemeinsame Diskussion,
    c. Feststellung und Sammlung problematischer Aspekte von Kriterienkatalog und KBP bei Anwendung in der Praxis,
    d. Vergleich mit anderen Vorgehensweisen aus Normen und Schemata, Diskussion und Entwicklung von Verbesserungsvorschlägen für Kriterien und KBP,
    e. Dokumentation der Auditergebnisse inhaltlich und verfahrenstechnisch.

3. Nachbereitung
    a. Erstellung der Auditdokumentation anhand des KBP,
    b. Überarbeitung erstellter Musterdokumente aufgrund von Feststellungen aus den durchgeführten Audits,
    c. Aufarbeitung der Auditergebnisse inhaltlich und verfahrenstechnisch,
    d. Durchführung von Feedbackrunden zu den Auditergebnissen (schriftlich und mündlich),
    e. Ableitung und Diskussion der Lessons Learned für das AUDITOR-Verfahren.

Die durchgeführten Pilotierungen haben die praktische Anwendbarkeit des Zertifizierungsverfahrenes bestätigt und darüber hinaus weiteres Verbesserungspotenzial aufgedeckt. Dieses Verbesserungspotenzial wurde von den Projektpartnern diskutiert und in das AUDITOR-Zertifizierungsverfahren zur Optimierung der bestehenden Dokumente eingearbeitet. Da kein europäisches Gütesiegel im Rahmen der Projektlaufzeit initiiert wurde, konnten keine Erprobungen mit europäischen Partnern, wie ursprünglich geplant, durchgeführt werden.

2.1.6. Standardisierung

Aufgabenbereich:	Standardisierung und Kriterienkatalog
Leitung:	DIN
Arbeitspakete gemäß GVB	• AP 3 • AP 5 Folgeantrag
Korrespondierende Teilziele	TZ5 Öffentlichkeitsarbeit, Zusammenarbeit mit anderen Stellen sowie Standardisierungsaktivitäten
Wesentliche Ergebnisse	• DIN SPEC 27557 • Vorbereitung der europäischen Normungsarbeit

Das Projekt hatte schließlich das Ziel, durch die Überführung der Projektergebnisse in eine DIN Spezifikation (DIN SPEC) den Transfer der im Laufe des Projektes erlangten Forschungsergebnisse in den Markt und die Praxis zu erleichtern und zu beschleunigen. Eine DIN SPEC kann als erster Schritt zur internationalen Normierung und Standardisierung verwendet werden. Normen als Zertifizierungsgrundlage haben sich in der Vergangenheit insbesondere bei der überregionalen und internationalen Anwendung bewährt und sind für die europaweite Anerkennung unerlässlich. Die Abbildung 5 zeigt schematisch den Prozess zur Erstellung einer DIN SPEC nach dem PAS-Verfahren, welcher im Rahmen des Projektes Anwendung gefunden hat. Nach der Festlegung des Prozesses zur Erstellung einer DIN SPEC durch das DIN wurde die Zusammenarbeit im Konsortium abgestimmt. Ein erstes zentrales Dokument stellt den Geschäftsplan dar, welcher unter anderem die Vorgehensweise zur Erstellung der DIN SPEC konkret für das AUDITOR-Projekt definiert.

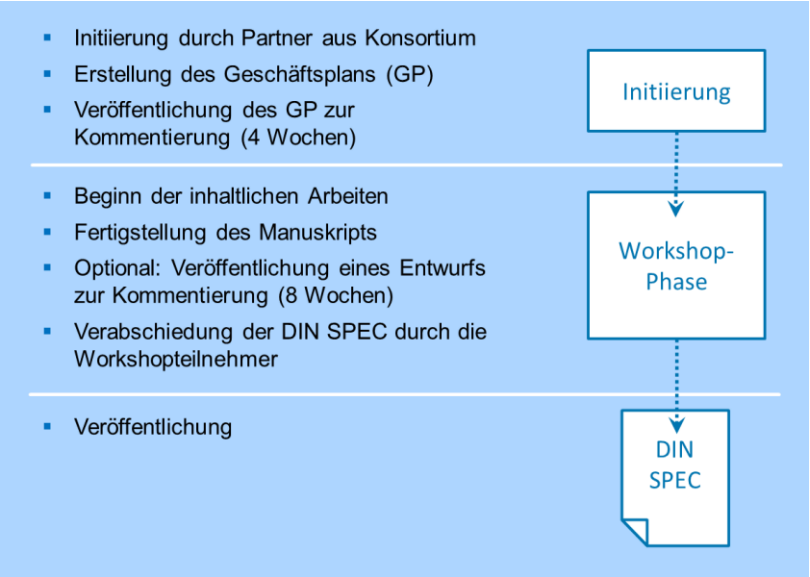

Abbildung 5. Prozess zur Erstellung einer DIN SPEC nach dem PAS-Verfahren[1]

[1] Abbildung angelehnt an https://www.din.de/de/forschung-und-innovation/din-spec/wie-eine-din-spec-entsteht-63574

Am 22.02.2019 wurde in Köln das erste Kick-off-Meeting der DIN-SPEC-Arbeitsgruppe durchgeführt. In dieser Arbeitsgruppe waren nicht nur Vertreter des AUDITOR-Konsortiums aktiv, sondern auch weitere Personen aus der Praxis (bspw. Vertreter von IBM). Im Sommer 2019 wurde die erste Fassung der DIN SPEC zur öffentlichen Kommentierung freigegeben. Die eingegangenen Kommentare wurden anschließend in einer gemeinsamen Web-Konferenz im Detail besprochen und aufgelöst. Da die DIN SPEC inhaltlich dem Kriterienkatalog entspricht, wurden die Erkenntnisse ebenfalls in den Kriterienkatalog zurückgeführt.

Die DIN-SPEC-Arbeitsgruppe entschied die Veröffentlichung der DIN SPEC erst nach Kommentierung und Bewilligung des AUDITOR-Kriterienkatalogs durch die Datenschutz-Aufsichtsbehörde LDI NRW und nach der Stellungnahme des EDSA im Rahmen des Bewilligungsprozesses durchzuführen. Damit ist sichergestellt, dass die DIN SPEC auch den Anforderungen der Datenschutz-Aufsichtsbehörden genügt. Aufgrund des langen Bewilligungsprozesses sowie umfassender Änderungen am Kriterienkatalog musste jedoch die DIN SPEC nahezu neu erstellt werden. Eine Veröffentlichung der DIN SPEC 27557 ist daher für Beginn 2025 vorgesehen.

Darüber hinaus wurde eine europäische Normungsarbeit vorbereitet, wodurch die DIN SPEC zukünftig zu einer Europäischen Norm (EN) weiterentwickelt werden kann. In enger Abstimmung mit dem DIN kann die DIN SPEC daher bei CEN/CENELEC zu einer Europäischen Norm weiterentwickelt werden. Diese Normierungsarbeiten ermöglichen ebenfalls eine Kommentierung und Berücksichtigung von Bedürfnissen und Anforderungen von europäischen Markteilnehmern.

2.1.7. Bewilligung des Zertifizierungsverfahrens

Aufgabenbereich:	Bewilligung des Zertifizierungsverfahrens
Leitung:	Karlsruher Institut für Technologie und Universität Kassel
Arbeitspakete gemäß GVB	• (Indirekt) AP 1, AP 2 und AP 5 • AP 1 Folgeantrag
Korrespondierende Teilziele	TZ4 Bewilligung
Wesentliche Ergebnisse	• Geschäftsmodell und Konzept zur Weiterführung des AUDITOR-Verfahrens • Genehmigung des AUDITOR-KBPs • Genehmigung des AUDITOR-Kriterienkatalogs, inkl. Stellungnahme des EDSA • Akkreditierung von datenschutz cert GmbH

Um eine nachhaltige Verwendung und weitreichende Verbreitung von AUDITOR sicherzustellen, wurden Anwendungskonzepte, Empfehlungen für ein nachhaltig erfolgreiches Zertifizierungsverfahren, und ein Geschäftsmodell für ein praktikables AUDITOR-Verfahren entwickelt und umgesetzt. Dabei wurden fortlaufend alle Akteure im Markt bei der Entwicklung der Zertifizierung eingebunden, deren Bedürfnisse verstanden, Interessen abgestimmt und im Projekt verankert. In Abstimmung mit allen Beteiligten am Markt wurde festgelegt, dass das Kompetenznetzwerk Trusted Cloud e.V. als Eigentümer des Zertifizierungsverfahren auftritt, da Trusted Cloud fundierte Erfahrungen im Themenkomplex Cloud Computing aufweist und bereits ein Gütesiegel für Cloud-Dienste anbietet. Trusted Cloud tritt als

Eigentümer und Verwalter auf, z.B. zur Pflege und Weiterentwicklung des Kriterienkatalogs. Die AUDITOR-Zertifizierung selbst kann jedoch von jeder akkreditieren Zertifizierungsstelle angeboten und durchgeführt werden. Der Konsortialpartner datenschutz cert wird als erste akkreditierte Zertifizierungsstelle die AUDITOR-Zertifizierung am Markt anbieten können.

Um die Akkreditierung von Zertifizierungsstellen zu ermöglichen, ist eine abgeschlossene nationale Bewilligung des AUDITOR-Zertifizierungsverfahrens zwingende Voraussetzung. Die Bewilligung umfasst sowohl die Aufnahme des AUDITOR-KBP in das Akkreditierungsprogramm der DAkkS sowie die Genehmigung des AUDITOR-Kriterienkatalogs durch die zuständige Datenschutz-Aufsichtsbehörde. Der Ablauf des Entwicklungs- und Bewilligungsprozess von Zertifizierungen ist in Abbildung 6 dargestellt.[2]

Abbildung 6. Schematische Darstellung des Entwicklungs- und Bewilligungsprozesses von Zertifizierungen.[3]

Zunächst prüfte die DAkkS das KBP auf Einhaltung entsprechender (europäischer und internationaler) Richtlinien zur Konformitätsbewertung, darunter insbesondere die ISO/IEC 17065 und ISO/IEC 17067. Die DAkkS übermittelte nach erfolgreicher (System-)Programmprüfung das AUDITOR-Zertifizierungsprogramm an die zuständige Datenschutz-Aufsichtsbehörde. Im Falle von AUDITOR war dies die LDI NRW.

Die Behörde prüfte zunächst alle relevanten Bestandteile des Zertifizierungsprogramms, insbesondere den Kriterienkatalog im großen Umfang. Dabei galt die Handreichung der DSK „Anforderungen an

---

[2] Die Details zum allgemeinen Verfahren können auch bei dem EDSA nachgelesen werden: https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en

[3] Grafik angelehnt und erweitert von https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf, der Deutschen Akkreditierungsstelle

datenschutzrechtliche Zertifizierungsprogramme“ als maßgebliche Grundlage zur Prüfung der Kriterien, da diese unter allen deutschen Aufsichtsbehörden abgestimmt wurde. Insofern die Aufsichtsbehörde Abweichungen oder Änderungsbedarf festgestellt hatte, wurden diese vom Konsortium in mehreren Iterationen umgesetzt. Abschließend übersendete die Aufsichtsbehörde den Prüfbericht der (Fach-)Programmprüfung über die Genehmigungsfähigkeit der Kriterien an die DAkkS.

Bevor eine Genehmigung der Zertifizierung abgeschlossen werden kann, muss jedoch auch noch der EDSA involviert werden. Der Prozess zur Einbindung sieht dabei eine informelle Konsultationsphase und eine formale Stellungnahme durch den EDSA vor. Die informelle Konsultationsphase fand einerseits zwischen den deutschen Datenschutz-Aufsichtsbehörden statt, welche die Möglichkeit erhielten, den Kriterienkatalog zu begutachten und zu kommentieren. Andererseits fand auch eine informelle Konsultation mit Vertreter: innen der europäischen Datenschutz-Aufsichtsbehörden und der Subgroup Compliance, E-Government & Health (CEH) statt. Hierzu wurden zwei Gutachter (Reviewer) bestellt, welche die englische Fassung des Kriterienkatalogs geprüft haben. Es wurden alle Änderungswünsche iterativ umgesetzt.

Nach Abschluss der informellen Konsultation wurde durch das LDI NRW das Stellungnahmeverfahren nach Art. 64 Abs. 1 lit. c DSGVO beantragt. Die Dauer des Verfahrens betrug 14 Wochen und endete mit einer Stellungnahme (‚Opinion‘) des EDSA zum Zertifizierungsprogramm, welche öffentlich einsehbar ist.[4] Die Opinion enthält Recommendations und Encourgements, welche umgesetzt wurden, bevor die (Fach-)Prüfung der Aufsichtsbehörde abgeschlossen und die Kriterien genehmigt werden konnten.

Nach Genehmigung der Kriterien hat die DAkkS die Akkreditierungsfähigkeit des Zertifizierungsprogramms formal festgestellt, sodass sich anschließend Zertifizierungsstellen nach dem Programm in Verbindung mit der ISO/IEC 17065 bei der DAkkS akkreditieren lassen können.

Die folgende Aufzählung fasst den langen und herausfordernden Bewilligungsprozess von AUDITOR zusammen:

- Februar 2020: Einreichung des Zertifizierungsprogramms bei der DAkkS.
- November 2020: Die DAkkS hat nach einer Überarbeitungsrunde das Zertifizierungsverfahren freigegeben und keine Mängel festgestellt, die einer Akkreditierung des Programms entgegenstehen können. Anschließend wurde das Zertifizierungsprogramm an die zuständige Datenschutz-Aufsichtsbehörde LDI NRW übermittelt.
- Januar 2022: Abschluss der Fachprüfung durch die LDI NRW. Die Aufsichtsbehörde hatte den Kriterienkatalog nach einer Überarbeitungsrunde freigegeben. Anschließend wurde das Zertifizierungsprogramm in die informelle Konsultationsphase auf der europäischen Ebene gegeben.

[4] https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks/auditor-conformity_de

- September 2022: Rückmeldung der europäischen Co-Reviewer zum Zertifizierungsverfahren.
- Im Verlauf von 2023: Fortlaufender Austausch mit LDI NRW zum Verfahrensstand. Einarbeitung von Feedback und Änderungswünschen durch europäische Reviewer (z.B. CNIL).
- In 2023: Klärung von offenen, Grundsatzfragestellungen zur Auslegung der Datenschutz-Grundverordnung, unter anderem in Bezug auf die sogenannte „Haushaltsausnahme“ im Anwendungskontext von Cloud-Diensten. Verschiedene Diskussionen durch die europäischen Datenschutz-Aufsichtsbehörden. Änderungswünsche wurden vom Konsortium adressiert.
- Frühjahr 2024: Einreichung von AUDITOR in den formalen Genehmigungsprozess bei dem EDSA durch das LDI NRW.
- Am 17.04.2024 hat der EDSA seine Stellungnahme (‚Opinion‘) zum AUDITOR-Kriterienkatalog formal abgegeben. Die Änderungsempfehlungen wurden vom Konsortium umgesetzt.
- Am 28.06.2024 hat das LDI NRW die Kriterien formal genehmigt. Die DAkkS führt seit dem 10.09.2024 AUDITOR als genehmigtes Zertifizierungsverfahren auf.

Damit ist der Bewilligungsprozess erfolgreich abgeschlossen. Zertifizierungsstellen am Markt können sich akkreditieren lassen und anschließend das AUDITOR-Verfahren anbieten. Der Konsortialpartner datenschutz cert hat bereits die Akkreditierung vorangetrieben und wartet auf Abschluss der Akkreditierung (*Stand Oktober 2024*). Die Vergabe von ersten Zertifikaten ist für Anfang 2025 vorgesehen (bspw. beim Konsortialpartner Cloud&Heat).

2.1.8. Kommunikation und Dissemination

Aufgabenbereich:	Begleitende Maßnahmen
Leitung:	Karlsruher Institut für Technologie
Arbeitspakete gemäß GVB	• AP 5, AP 6, AP 8, AP 9 • AP 6 Folgeantrag
Korrespondierende Teilziele	TZ5 Öffentlichkeitsarbeit, Zusammenarbeit mit anderen Stellen sowie Standardisierungsaktivitäten
Wesentliche Ergebnisse	• Empfehlungen zur Nachhaltigkeit und Anwendbarkeit des Datenschutzzertifikats • Konzept für Übergangsszenario TCDP • Bekanntheit von AUDITOR bei relevanten Stakeholdern • Publikationen, Vorträge, Messebesuche, Newsartikel

Als wichtige Nebenaufgabe führte das Konsortium die kontinuierliche Evaluation und Verbreitung der Teilergebnisse sowie die Kommunikation mit dem Projektträger und Zuwendungsgeber und weiteren wichtigen Stakeholdern durch, insbesondere mit Datenschutz-Aufsichtsbehörden, Cloud-Anbietern, Zertifizierungsstellen, Cloud-Kunden und europäischen Interessengruppen.

Das Konsortium führt regelmäßige Telefonkonferenzen zur besseren Abstimmung durch. Es wurde ein interner und externer E-Mail-Verteiler eingerichtet, um sowohl Konsortialpartner (interner Verteiler) als auch Projektinteressierte und assoziierte Partner (externer Verteiler) fortlaufend zu informieren. Zudem wurde eine deutschsprachige und englischsprachige Website für das Projekt erstellt (www.auditor-cert.de und www.auditor-cert.eu) und fortlaufend gepflegt. Auch wurde ein Newsletter für das Projekt etabliert, welcher anlassbezogen Informationen an mehr als 230 Abonnenten verteilte. Der Newsletter kann auf der Webseite von jedem interessierten Internetnutzer abonniert werden.

Das KIT organisierte gemeinsam mit der Universität Kassel, TrustedCloud und dem BMWK den Lenkungsausschuss von AUDITOR. Dieser tagte in unregelmäßigen Zeitabständen und sorgte für die politische und inhaltliche Abstimmung von AUDITOR. Darüber hinaus organisierte das KIT gemeinsam mit der Universität Kassel und TrustedCloud den Expertenbeirat von AUDITOR. Dieser tagte in unregelmäßigen Zeitabständen und sorgte für inhaltliche Abstimmung von AUDITOR.

Über die gesamte Projektlaufzeit hinweg wurden verschiedene Maßnahmen zur Kommunikation und Dissemination durchgeführt, welche im Folgenden kurz zusammengefasst werden.

Öffentlichkeitsarbeit zur Erhöhung der Bekanntheit und Reputation

Im Allgemeinen strebte das AUDITOR-Projekt eine breite Nutzung der Zertifizierung an. Aus diesem Grund wurden alle Teilnehmer am Markt, insbesondere Zertifizierungsstellen, Cloud-Anbieter und -Kunden sowie Datenschutz-Aufsichtsbehörden frühzeitig in das Projekt involviert. Durch vielfältige und internationale Workshops, Web-Sessions sowie Messe-Auftritte (z.B. CEBIT, Cloud Expo; siehe Abbildung 7) wurde nicht nur die Bekanntheit der eingetragenen Marke „AUDITOR“ erhöht, sondern das Projekt konnte auch fortlaufend Feedback zur Zertifizierung erhalten und berücksichtigen. Flankierend wurden eine Vielzahl von Zeitschriftenartikel veröffentlicht, Interviews gegeben, und (elektronische) Handreichungen und Online-Videos produziert (siehe auch Kapitel 2.6).

Abbildung 7. AUDITOR Messestand auf der CEBIT 2018

Durch diese Veranstaltungen konnten im Verlaufe der Projektlaufzeit weitere assoziierte Partner gewonnen werden, welche den Kriterienkatalog und das KBP hinsichtlich der Anwendbarkeit in ihrem konkreten Unternehmen evaluiert haben. Die Ergebnisse dieser Prüfung wurden mit dem AUDITOR-Konsortium jeweils diskutiert, sodass fortlaufende Verbesserungen am Zertifizierungsverfahren zur Sicherstellung der Anwendbarkeit durchgeführt wurden. Der Webauftritt zur Kommunikation der Ergebnisse wurde fortlaufend aktualisiert (www.auditor-cert.de /.eu), um den Projektfortschritt und die Ergebnisse der breiten Öffentlichkeit zugänglich zu machen, darunter auch ein Wiki zum Kriterienkatalog samt Kommentarfunktionen.

Da AUDITOR auf dem TCDP aufbaut, wurde zudem die Übertragbarkeit des TCDP auf AUDITOR diskutiert und eruiert. Es ist im Interesse des Markterfolgs der AUDITOR-Zertifizierung, jene Unternehmen, die durch die TCDP-Zertifizierung ihrer Cloud-Dienste bereits hohe Bereitschaft bewiesen haben, zu AUDITOR zu überführen. Zudem kann dadurch die Markakzeptanz von AUDITOR erhöht werden. Hierzu wurden u.a. Änderungen an dem TCDP vorgeschlagen und die TCDP-zertifizierten Unternehmen kontaktiert und informiert.

Ansprache von Akteuren zur Sicherstellung der Marktakzeptanz

Zertifizierungsstellen am Markt wurden aktiv angesprochen und über die Bedingungen zur Durchführung von Zertifizierungen informiert. Cloud-Anbieter wurde der Kriterienkatalog vorgestellt sowie die Lessons Learned aus den drei Pilotierungen präsentiert.

Bemerkenswert ist zudem die freiwillige Unterstützung durch assoziierte Partner bei der Vermarktung von AUDITOR. So wurde bspw. auf Eigeninitiative der Deutschen Telekom und Salesforce eine neue Arbeitsgruppe gemeinsam mit dem BMWK geschaffen, welche bereits früh im Projekt Marketing- und Transfermaßnahmen entwickelt und besprochen hat. Zum Beispiel wurde die Fertigstellung des AUDITOR-Kriterienkatalogs bei einem öffentlichen Pressetermin im Hause des BMWK vorgestellt (siehe Abbildung 8).

Abbildung 8. Pressekonferenz im BMWK.

Auch international wurden verschiedene Akteure angesprochen und in das Projekt involviert. So wurde AUDITOR bei der EU-Kommission vorgestellt und ein Workshop in Brüssel sowie weitere Web-Sessions mit europäischen Datenschutz-Aufsichtsbehörden durchgeführt. Eine Anerkennung von AUDITOR auf europäischer Ebene führt zum einen zu einer erhöhten Marktakzeptanz, zum anderen schafft es die Möglichkeiten AUDITOR zu einem europäischen Gütesiegel weiterzuentwickeln.

Nationaler und internationaler Austausch mit politischen Akteuren

Das Forschungsprojekt hat bereits bei Beginn der Entwicklung die zentralen politischen Stakeholder für das Zertifizierungsverfahren konsequent eingebunden. Besonders hervorzuheben ist bspw. die Vorstellung von AUDITOR bei den Datenschutz-Aufsichtsbehörden. Bereits im Jahr 2019 wurde ein exklusives Treffen mit dem (ehemaligen) BfDI Ulrich Kelber und Vertretern des BfDI in Bonn durchgeführt (siehe Abbildung 9). Das BfDI hatte dem AUDITOR Projektteam unter anderem die Unterstützung auf internationaler Ebene zugesichert. Besonders hervorzuheben ist ebenfalls die Vorstellung bei der LDI NRW im Juni 2019 in Düsseldorf. Des Weiteren stand das AUDITOR Projekt mit weiteren nationalen Datenschutz-Aufsichtsbehörden in Kontakt, um den Austausch über aktuelle Entwicklungen und auch die Transparenz der Projektergebnisse sicherzustellen. AUDITOR war auch das einzige Pilotprojekt im Themenfeld der Datenschutzzertifizierungen der DAkkS. Neben den nationalen Aktivitäten wurde AUDITOR mehrfach auf europäischer Ebene in unterschiedlichen Institutionen in Brüssel vorgestellt und auf Roadshows in Kanada und Japan präsentiert.

Abbildung 9. AUDITOR Projekt beim ehemaligen BfDI Kelber.

Einbindung wichtiger Cloud-Anbieter

Für Cloud-Anbieter bietet die AUDITOR-Zertifizierung eine zentrale Differenzierungsmöglichkeit gegenüber Wettbewerbern, da sie mit dem AUDITOR-Zertifikat die Einhaltung der Vorgaben der Datenschutz-Grundverordnung nachweisen und im Cloud-Dienst-Markt ein national gültiges Zertifikat vorweisen können. Das Projekt wird bereits durch eine Vielzahl von namenhaften Cloud-Anbietern unterstützt, darunter bspw. IBM, Salesforce, Deutsche Telekom, und SAP. Aber auch viele KMU Cloud-

Anbieter haben das Projekt fortlaufend begleitet (siehe Kapitel 1.5). So wurden Projekttreffen nicht nur von Projektpartnern, sondern auch von vielen interessierten Stakeholdern besucht (siehe Abbildung 10). Gerade im Cloud-Markt ist es zudem von höchster Relevanz, dass die sogenannten Hyperscaler auch die AUDITOR-Zertifizierung anerkennen und sich danach zertifizieren lassen, da viele Unternehmen wiederrum ihre Dienste auf den Plattformen der Hyperscaler betreiben. AUDITOR ist daher fortlaufend insbesondere mit Microsoft, Amazon und Google im Austausch. Aus Gesprächen mit Cloud-Anbietern und -Kunden zeigt sich, dass der Bedarf an einer Datenschutzzertifizierung für Cloud-Dienste weiterhin gegeben ist.

Abbildung 10. AUDITOR Projekttreffen in Karlsruhe

2.2. Wichtigste Positionen des zahlenmäßigen Nachweises

Zur Durchführung des Projektes wurden im wesentlichen Personalmittel benötigt. Darüber hinaus umfasst der zahlenmäßige Nachweis Sachmittel und Reisekosten zur Durchführung von Workshops, Öffentlichkeitsarbeit und ähnlicher Aktivitäten. Um zusätzliche Expertise in das Konsortium einfließen zu lassen, haben unter anderem Trusted Cloud, VOICE und das ULD als assoziierte Partner das Konsortium unterstützt. Darüber hinaus hat Hornetsecurity als assoziierter Partner eine Erprobung von AUDITOR durchgeführt und das Projekt fortlaufend unterstützt. Zur Einbindung dieser Partner wurden entsprechende Unteraufträge vergeben. Ferner stellte die Vergabe von Aufträgen an die Gutachter aus ausgewählten europäischen Mitgliedstaaten einen ebenfalls relevanten Posten dar. Für weitere Details wird auf die Finanzberichte der Partner verwiesen.

2.3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die in den einzelnen Arbeitspaketen durchgeführten Arbeiten sowie die Förderung waren notwendig und angemessen. Die interdisziplinäre Herangehensweise für die Entwicklung eines (nationalen) DSGVO-konformen Zertifizierungsverfahrens hat sich im Projektverlauf als angemessen und fruchtbar erwiesen.

Alle Arbeitspakete und entsprechende Arbeiten des Konsortiums wurden so durchgeführt, dass die vielen Anforderungen der DAkkS sowie nationaler und europäischer Aufsichtsbehörden zur Entwicklung und Genehmigung einer Datenschutzzertifizierung vollends eingehalten wurden. Da Art. 42 und Art. 43

DSGVO rechtlich bindende Anforderungen an Datenschutzzertifizierungen vorgeben, waren alle Projekttätigkeiten auf deren Erfüllung ausgerichtet. Parallel waren Kommunikations- und Disseminationsarbeiten dringend notwendig, um die Marktakzeptanz und die nachhaltige Anwendung von AUDITOR sicherzustellen.

Im AUDITOR-Forschungsprojekt wurden grundlegende Fragestellungen zur Entwicklung von Datenschutzzertifizierungen erarbeitet und gelöst. Die Ergebnisse orientierten sich einerseits an die Anforderungen des Cloud-Markets. Dadurch wurden alle Spezifika von Cloud-Diensten bei der Zertifizierung berücksichtigt. Gerade diese kontextuelle Betrachtung war zielführend, da vergleichbare Zertifizierungen (bspw. EuroPriSe) sich allgemein auf die Zertifizierung von Auftragsverarbeitungsverhältnissen fokussieren. Zudem haben die Diskussionen der Aufsichtsbehörden in Bezug auf die Haushaltsausnahme während des Bewilligungsprozesses gezeigt, dass einige Unklarheiten bei der Auslegung der Datenschutz-Grundverordnung vorlagen. Diese wurde durch AUDITOR aufgedeckt und von den Aufsichtsbehörden aufgelöst.

Die Förderung des Projektes ist zudem im Einklang mit der Datenschutz-Grundverordnung, welche in Art. 42 Abs. 1 gerade solch eine Förderung vorsieht: „*Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird*“.

Der Erfolg von Zertifizierungsangeboten in der IT-Branche hängt grundsätzlich davon ab, ob der Aufwand der Zertifizierung in einem positiven Zusammenhang mit internen Kostenreduktionen oder zunehmender Marktattraktivität steht. Für eine Datenschutzzertifizierung waren diese Aspekte allerdings noch schwerer zu fassen, da zum einen die Datenschutz-Grundverordnung erstmals die Grundlagen für eine solche Zertifizierung schafft. Zum anderen war nicht klar, wie hoch der wahrgenommene Nutzen durch das zertifizierte Unternehmen gegenüber bereits bestehenden Zertifizierungen ist (bspw. ISO/IEC 27001). Ein weiteres Risiko stellte das Aufkommen bzw. die Änderungen der rechtlichen Rahmenbedingungen dar, welches eine kontinuierliche Anpassung der Zertifizierungsprozesse erforderte. Die Partner des Vorhabens AUDITOR konnten Forschungsrisiken in geringerem Umfang selbst tragen, waren aber zur Abfederung von technischen und wirtschaftlichen Risiken auf kooperative Arbeitsweisen und entsprechende Forschungsförderung angewiesen. Die Förderung eines Forschungsprojektes und die Durchführung von Aktivitäten zur Erforschung und Entwicklung einer Zertifizierung scheint unter Berücksichtigung dieser Punkte daher angemessen.

Besonders hervorzuheben sei der komplexe und lang andauernde Bewilligungsprozess der Zertifizierung. AUDITOR war in Deutschland, gemeinsam mit EuroPriSe, die erste Zertifizierung, die solch einen Prozess durchlaufen hat. Damit hat AUDITOR eine Vorreiterrolle eingenommen und den Weg für weitere Zertifizierungsverfahren geebnet. Auf der anderen Seite musste AUDITOR auch Unsicherheiten, Unklarheiten sowie fehlende Prozessspezifikationen und Verantwortlichkeiten im Rahmen des Bewilligungsprozesses überwinden. Mit einer kleineren Forschungsgruppe oder weniger

Investitionsmitteln wäre der Bewilligungsprozess nicht durchführbar gewesen. Da AUDITOR schlussendlich sein maßgebliches Ziel erreicht hat und die Datenschutzzertifizierung durch die zuständige Datenschutz-Aufsichtsbehörde und die DAkkS bewilligt wurde, war die Förderung und die geleisteten Arbeiten notwendig und angemessen. AUDITOR ist zum aktuellen Zeitpunkt in Europa die einzige Datenschutzzertifizierung für Cloud-Dienste.

2.4. Voraussichtlicher Nutzen, insbesondere Verwertbarkeit der Ergebnisse

Die Breitenwirkung und Verwertbarkeit des Projekts sind als sehr hoch anzusehen, da die Thematik einen großen Interessenkreis besitzt. Die zu Projektbeginn stattfindenden Umwälzungen im Datenschutzrecht haben zu einer großen Verunsicherung bei Cloud-Dienst-Kunden aber auch -Anbietern geführt. Neue Pflichten verbunden mit einem hohen Sanktionsrisiko lassen Zertifizierungen neue Attraktivität zukommen.

Die Datenschutzzertifizierung AUDITOR nach Maßgabe der Datenschutz-Grundverordnung ist im Interesse aller Beteiligten des Cloud-Markts, insb. von Cloud-Kunden und Betroffenen, Cloud-Anbietern und Zertifizierungsstellen. Abbildung 11 fasst das Wertschöpfungsnetzwerk von AUDITOR zusammen und Abbildung 12 stellt die wichtigsten Vorteile von AUDITOR dar.

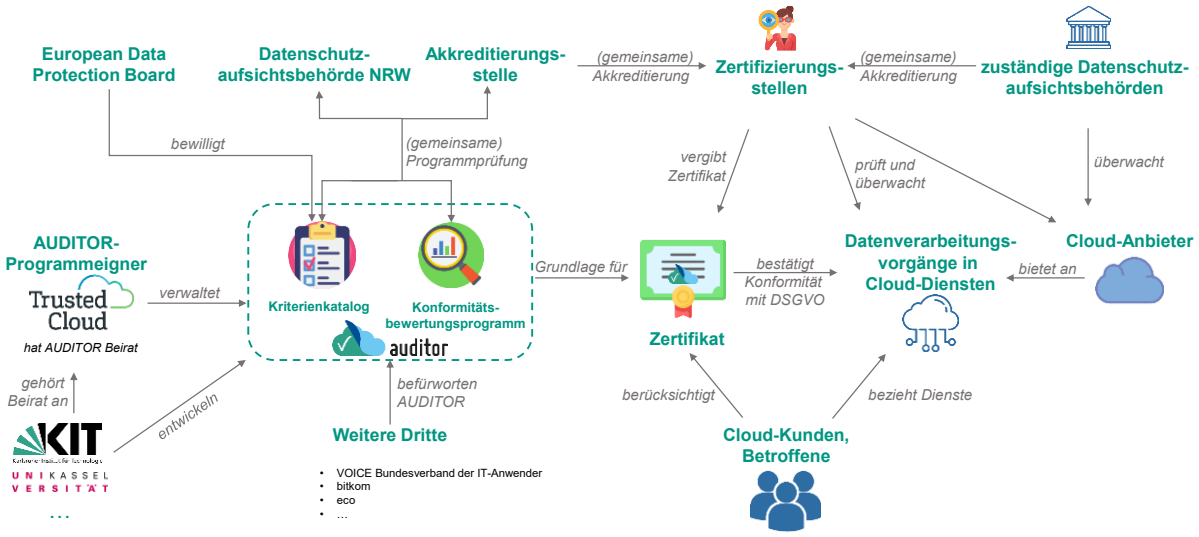

Abbildung 11. AUDITOR Wertschöpfungsnetzwerk[5]

[5] Abbildung eigene Darstellung. Icons von der Website: https://www.flaticon.com/

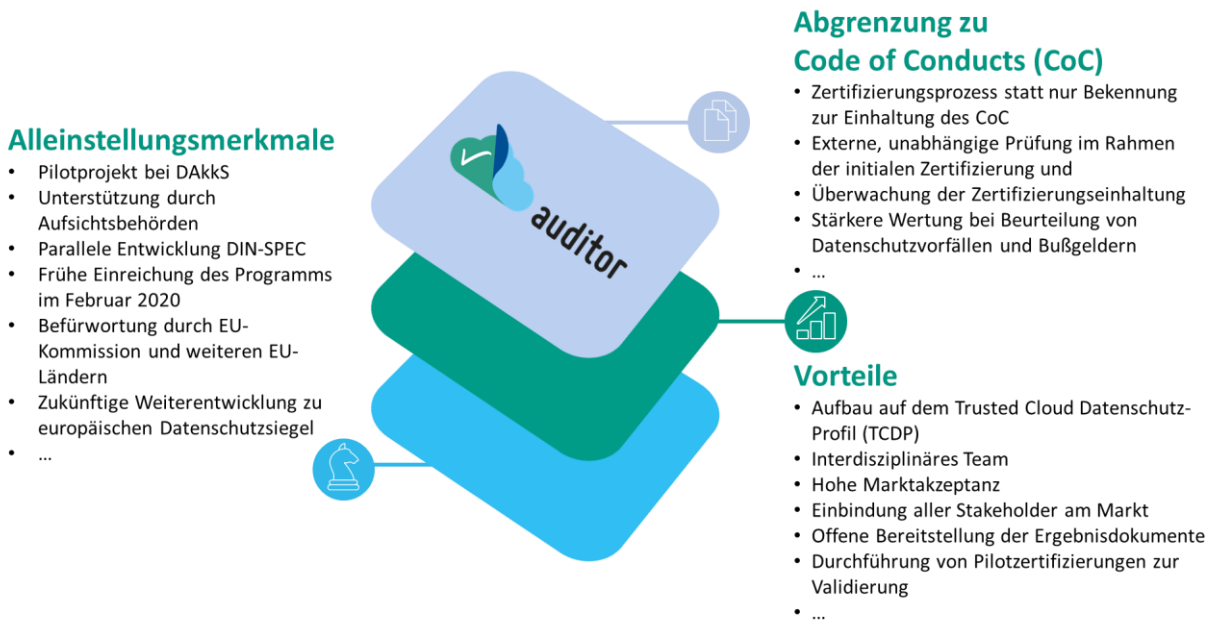

Abbildung 12. Zusammenfassung der wichtigen Vorteile von AUDITOR

2.4.1. Der Nutzen Für Cloud-Kunden: Sicherheit und Transparenz

In Europa ansässige Cloud-Kunden dürfen nur mit solchen Cloud-Anbietern zusammenarbeiten, die hinreichend Garantien zur Einhaltung des Datenschutzes vorweisen können. Allerdings können Cloud-Kunden kaum beurteilen, ob der Cloud-Anbieter tatsächlich alle für die Verarbeitungsvorgänge des Cloud-Dienstes relevanten Anforderungen nach der Datenschutz-Grundverordnung erfüllt. Nach Art. 42 DSGVO ist eine genehmigte Datenschutzzertifizierung wie AUDITOR ein wichtiges Mittel zum Nachweis der Einhaltung und schafft damit Rechtssicherheit und unterstützt Kunden bei der Auswahl von Cloud-Diensten. Schließlich stellt die Nutzung von Cloud-Diensten in der Regel eine Auftragsverarbeitung dar und der Cloud-Kunde bleibt als Verantwortlicher für die ausgelagerte Datenverarbeitung verantwortlich. Cloud-Kunden können die AUDITOR-Zertifikate dann wiederrum ihren (End-)Nutzern vorlegen und nachweisen, dass sie einen rechtskonformen Cloud-Dienst nutzen.

Gerade Datenschutzzertifizierungen wie AUDITOR können zudem bestehende (abstrakte) Richtlinien zur Auswahl von datenschutz-konformen Cloud-Lösungen unterstützen, indem sie keine pauschalen Empfehlungen über den Einsatz von Cloud-Diensten geben, sondern vielmehr für jeden Dienst einzeln angeben, ob dieser Dienst konform zur Datenschutz-Grundverordnung ist. Entscheidungsbeauftragte werden daher bei dem Vergleich und der Auswahl von konkreten Diensten besser und zielgenau unterstützt. Zertifizierungen wie AUDITOR können dann auch als globaler Mechanismus zur dezentralen Selbstregulierung dienen. Der Wettbewerbsdruck kann Unternehmen dazu motivieren, Standards für die Datenverwaltung und den Datenschutz einzuführen und sich entsprechenden Zertifizierungen zu unterziehen, auch wenn diese nicht ausdrücklich durch Vorgaben vorausgesetzt werden.

Betroffene von Datenverarbeitungsvorgänge werden durch eine unabhängige Überprüfung durch eine Zertifizierungsstelle besser geschützt, da mögliche Sicherheitsschwachstellen oder fahrlässige Verarbeitungstätigkeiten aufgedeckt werden und Cloud-Anbieter Best-Practices umsetzen können. AUDITOR kann auch dazu beitragen, die asymmetrische Machtverteilung zwischen Einzelpersonen und Unternehmen zu verringern, indem sie Transparenz über Datenverarbeitungspraktiken schaffen und den Einzelnen in die Lage versetzen, besser informierte Entscheidungen zu treffen. So bereitete es in der Vergangenheit Nutzern immer wieder Probleme, die Authentizität von Gütesiegeln und Zertifikaten zu prüfen. Nutzer werden immer wieder in den Medien vor „Fake“-Siegeln gewarnt, die durch böswillige Anbieter eigenständig entworfen und auf Internetseiten zu Werbezwecken platziert werden. Denn durch die übliche Darstellung von Zertifikaten als einfache, grafische Gütesiegel ist es Anbietern ein Leichtes, diese nachzubauen und auf ihren Internetseiten zu nutzen. Ebenfalls gibt es regelmäßig Berichte über abgelaufene Zertifikate, die dennoch zu Werbezwecken auf den Internetseiten ausgewiesen werden. Die Nutzer haben jedoch oft nicht die Möglichkeit, die Gültigkeit der Zertifikate eigenständig prüfen zu können, weil es kein zentrales Verzeichnis gibt, das darüber Auskunft geben könnte. AUDITOR kann zur Adressierung dieser Probleme beitragen, indem AUDITOR auf Basis einer fachlich geeigneten und unabhängigen Prüfung und durch regelmäßige Kontrollen verlässliche Aussagen zur Datenschutzkonformität von Datenverarbeitungsvorgängen in digitalen Diensten trifft. AUDITOR legt mit den klaren Anforderungen an den Zertifizierungsprozess und akkreditierten Zertifizierungsstellen damit einen Grundstein für ein verlässliches Zertifizierungssystem und für vertrauenswürdige Anbieter. Auf diese Weise können Zertifizierungen dabei helfen, Bedenken bei Nutzern abzubauen und Vertrauen und Transparenz am Markt zu steigern.

2.4.2. Der Nutzen für Cloud-Anbieter: Vertrauensmechanismus, Wettbewerbsvorteil, interne Verbesserungen

Auch Cloud-Anbietern verspricht eine AUDITOR-Zertifizierung eine Vielzahl von Vorteilen. So können Zertifikate helfen das Kundenvertrauen in die angebotenen Cloud-Dienste zu steigern. Mit einer Zertifizierung kann ein Anbieter nachweisen, dass er alle datenschutzrechtlichen Anforderungen einhält. Tatsächlich sind Zertifizierungen (Art. 42 DSGVO) neben anerkannten Verhaltensregeln (Art. 40 DSGVO) die einzigen Instrumente, um die Konformität zur DSGVO (rechtssicher) nachweisen zu können (vgl. Art. 5 Abs. 2, 24 Abs. 3, 25 Abs. 3 DSGVO).

Zertifizierungen schaffen Transparenz, erhöhen die Vergleichbarkeit von Systemen und helfen dem Kontrollverlust von Nutzenden entgegenzuwirken. Verfügt der Cloud-Anbieter über ein anerkanntes AUDITOR-Zertifikat, kann er dieses auch für Marketingzwecke einsetzen. Auf diese Weise können zertifizierte Cloud-Anbieter Wettbewerbsvorteile gegenüber anderen Cloud-Anbietern erzielen.

Zudem bestehen gerade bei KMU weiterhin große Unsicherheiten, wie die abstrakten Anforderungen der Datenschutz-Grundverordnung umgesetzt werden sollen. Die AUDITOR-Zertifizierung trägt gerade zum Abbau dieser Unsicherheiten bei, denn es definiert die Anforderungen speziell an Cloud-Dienste und gibt Umsetzungshinweise, wie einzelne Kriterien durch technisch-organisatorische Maßnahmen in

das Unternehmen eingebettet werden können. Dafür werden auch Best-Practices zur Umsetzung der Zertifizierungskriterien vorgeschlagen oder auf anerkannte Standards und Industrienormen verwiesen.

Weiterer Vorteil für die Anbieter ist es, dass die Aufsichtsbehörde die Einhaltung von genehmigten Zertifizierungsverfahren als mildernden Faktor bei der Verhängung von Geldbußen gem. Art. 83 Abs. 2 lit. j DSGVO berücksichtigen muss.

2.4.3. Der Nutzen für Zertifizierungsstellen: Neue Gewinnpotenziale

Auch für Zertifizierungsstellen, für deren Geschäftsfeld die Datenschutz-Grundverordnung zwingende Regeln vorsieht, schafft die AUDITOR-Zertifizierung neue Chancen vertrauenswürdige Beratungs- und Prüfleistungen am Markt anzubieten. Nach erfolgreicher Akkreditierung können Zertifizierungsstellen das AUDITOR-Verfahren am Markt anbieten und so neue Gewinnpotenziale erschließen. Bei einer Laufzeit einer Zertifizierung von drei Jahren sowie jährlichen Überwachungsaudits ist bei einer weitreichenden Markakzeptanz ein hoher Umsatz der Zertifizierungsstellen zu erwarten. Weitere Prüfstellen können sich ebenfalls akkreditieren lassen, um spezielle Teilprüfungen zu übernehmen und somit ebenfalls ihr Angebotsportfolio zu erweitern. So wäre bspw. denkbar, dass eine Prüfstelle nach ISO/IEC 17021 akkreditiert ist und daher Auditierungen im Rahmen des AUDITOR-Verfahrens als ausgegliederte Prüfstelle durchführen kann.

Schließlich werden auch Zertifizierungsstellen unterstützt, indem mit dem KBP nicht nur ein offenes und klares Regelwerk zur Durchführung der Zertifizierung entwickelt wurde, sondern auch pro Zertifizierungskriterium angegeben wird, welche Prüfmethoden zum Einsatz kommen können. Dies gibt den Zertifizierungsstellen eine bessere Anleitung und erhöht die Vergleichbarkeit von Prüfungen.

2.4.4. Weitreichender Einfluss und Auswirkungen von AUDITOR

Darüber hinaus bietet die AUDITOR-Zertifizierung Vorteile für weitere Akteure am Markt, wie Datenschutz-Aufsichtsbehörden, die bei der Beurteilung von Cloud-Diensten unterstützt werden, oder Anbieter von komplementären Produkten, wie dem IT-Sicherheits-Kriterienkatalog C5 des BSI. Die AUDITOR-Zertifizierung wird auch eine wesentliche Rolle bei dem wegweisenden Projekt Gaia-X zur Schaffung einer vernetzten Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems einnehmen. Der Nachweis der Konformität zur Datenschutz-Grundverordnung ist ein wichtiges Kriterium für Cloud-Dienste, die zukünftig auf der Gaia-X Dateninfrastruktur angeboten werden. Auf dem Markt für Cloud-Dienste besteht daher ein großes Interesse an der AUDITOR-Datenschutzzertifizierung.

AUDITOR hat auch weitreichende Auswirkungen auf die Entwicklung von zukünftigen Datenschutzzertifizierungen. Als eine der ersten Datenschutzzertifizierungen wurde durch AUDITOR ein Referenzmodell konzipiert, welches für die Entwicklung weiterer Zertifizierungen als Grundlage dient. Anfängliche, widersprüchliche Diskussionen über den Zertifizierungsgegenstand und die Unsicherheiten bei der Entwicklung eines Kriterienkatalogs oder der Festlegung von Regeln für Zertifizierungsstellen hat das AUDITOR-Projekt überwunden und schafft Hilfestellungen für den Markt durch die transparente Bereitstellung aller Ergebnisse und Lessons Learned. So baut das

Schwesterprojekt DIRECTIONS maßgeblich auf den Ergebnissen von AUDITOR auf, um eine Datenschutzzertifizierung für schulische Informationssysteme zu entwickeln, damit Unsicherheiten im Bildungswesen reduziert und die Nutzung von digitalen Tools im Schulalltag gefördert werden können.[6]

Schließlich hat AUDITOR auch den Anstoß gegeben, ungeklärte Auslegungen des Datenschutzrechts aufzulösen. So wurde im Rahmen des Bewilligungsprozesses festgestellt, dass die europäischen Aufsichtsbehörden ein unterschiedliches Verständnis über die Nutzung von Cloud-Diensten für die private Datenverarbeitung und die Rolle von Zertifizierungen haben (Stichwort „Haushaltsausnahme“ der Datenschutz-Grundverordnung). AUDITOR hat stehts auch die Zertifizierung von Cloud-Diensten für private Endkunden fokussiert (z.B. die private Nutzung von Dropbox). Diese Ansicht hat dazu geführt, dass die europäischen Aufsichtsbehörden mehrere Komitees mit entsprechenden Grundsatzfragestellungen zur Klärung beauftragt haben. AUDITOR hat damit zum Abbau von Unsicherheiten bei der Rechtsauslegung der Datenschutz-Grundverordnung beigetragen.

2.4.5. Fortlaufende Maßnahmen und Mechanismen zur Sicherstellung der Nutzbarkeit und Verwertbarkeit

Die Nutzbarkeit und Verwertbarkeit der Datenschutzzertifizierung für die zentralen Akteure wurden von Anfang an durch geeignete Maßnahmen sichergestellt. Damit Cloud-Kunden und Endnutzer die Zertifizierung verstehen und Einsicht erhalten können, wurden aussagekräftige Gütesiegel und Zertifikatsdarstellungen entworfen. Im Gegensatz zu vielen bestehenden Zertifikaten sollen gerade relevante Informationen (z.B. über den Umfang der Zertifizierung) dem Kunden vermittelt werden. Hierzu wurden auch begleitende wissenschaftliche Studien durchgeführt (siehe Kapitel 2.6).

Ebenfalls wurde sichergestellt, dass sich möglichst viele Cloud-Anbieter nach AUDITOR zertifizieren lassen können. Neben den Hilfestellungen für Cloud-Anbieter, bspw. in Form von Umsetzungshinweisen im Kriterienkatalog, wurde ein Modularisierungskonzept entworfen. Dieses enthält zwei wesentliche Bestandteile: ein Schutzklassenkonzept und die Anerkennung bestehender Zertifizierungen (siehe Kapitel 2.1.4). Das Schutzklassenkonzept berücksichtigt, dass nicht jede Datenverarbeitung in einem Cloud-Dienst im gleichen Maß kritisch oder gefährdet ist. Daher kann ein Cloud-Anbieter zwischen normalem, hohen, und sehr hohem Schutzbedarf wählen und seine Cloud-Dienste entsprechend zertifizieren lassen. Jede Schutzklasse hat einen anderen Umfang an zu prüfenden Kriterien. Damit soll auch eine Zertifizierung für KMU erschwinglich sein, welche nur einen normalen Schutzbedarf benötigen. Auch berücksichtigt das Modularisierungskonzept den Umstand, dass Cloud-Dienste oft aufeinander aufbauen. Wird z.B. eine zertifizierte Cloud-Plattform genutzt, um eigene Anwendungen darauf zu betreiben, so muss nur die Anwendung zertifiziert werden und nicht erneut die darunter liegende Plattform. Dies spart Kosten und reduziert den Mehraufwand durch doppelte Prüfungen in verschachtelten Cloud-Umgebungen.

---

[6] Siehe hierzu www.directions-cert.de. Gefördert durch das Bundesministerium für Bildung und Forschung. FKZ: 01PP21003

2.4.6. Sicherstellung der breiten Anwendbarkeit von AUDITOR

Der wirtschaftliche Erfolg wurde im Forschungsprojekt von Anfang an fokussiert und mit geeigneten Maßnahmen unterstützt. Als Vermarkter und Eigner wurde Trusted Cloud festgelegt. Trusted Cloud besitzt nicht nur bereits etablierte organisatorische Strukturen, Expertise, Bekanntheit und einen guten Ruf im Cloud-Umfeld. Sondern sie haben die Entwicklung von AUDITOR maßgeblich begleitet und leiteten den Bewilligungsprozess.

Alleinstellungsmerkmal von AUDITOR ist, dass Trusted Cloud jeder akkreditierten Zertifizierungsstelle die eigene Vermarktung und Durchführung von AUDITOR-Zertifizierungen ermöglicht. Im Gegensatz zu anderen Datenschutzzertifizierungen (bspw. EuroPriSe) wird AUDITOR daher grundsätzlich zu nicht-diskriminierenden Bedingungen am Markt zur Verfügung gestellt werden. Dies bedeutet auch, dass das AUDITOR-Zertifizierungsverfahren gleichzeitig durch verschiedene Zertifizierungsstellen angeboten wird. Zum aktuellen Zeitpunkt lassen sich datenschutz cert GmbH und PwC Certification Services GmbH akkreditieren, sodass diese AUDITOR vorrausichtlich Ende 2024 am Markt anbieten können. Weitere Zertifizierungsstellen haben das Projekt fortlaufend begleitet und ihr Interesse geäußert (bspw. DEKRA, TÜV-Gruppe, ePrivacy).

Trusted Cloud hat ein Geschäftsmodell und insb. ein Lizenzmodell entwickelt, welches die Kosten für die Pflege, Weiterentwicklung und Marktansprache deckt. Dazu zählen bspw. jährliche Lizenzgebühren sowie Gebühren pro vergebenem Zertifikat durch eine Zertifizierungsstelle. Diese Lizensierung des AUDITOR-Zertifikats ist gerade im Cloud-Umfeld unabdingbar, denn es gibt eine große Menge an Cloud-Anbietern, deren Bedarf durch einzelne Zertifizierungsstellen nicht gedeckt werden kann. Somit werden lange Wartezeiten und Engpässe bei Zertifizierungsstellen reduziert. Zudem haben die meisten Cloud-Anbieter bereits langjährige Verträge mit Zertifizierungsstellen und wollen daher Zertifizierungsstellen nicht wechseln. Auch zielt AUDITOR mit der öffentlichen Verfügbarkeit der Zertifizierung darauf ab, die Kosten der einzelnen Zertifizierungen zu reduzieren, da die Zertifizierungsstellen im Markt im gegenseitigen Wettbewerb stehen und somit sich auch durch Zertifizierungskosten zukünftig differenzieren müssen. Von den geringeren Kosten profitieren nicht nur Cloud-Anbieter, für die Zertifizierungen dadurch vielleicht gerade erst erschwinglich werden, sondern auch indirekt Cloud-Kunden, die geringe Gebühren für die Cloud-Nutzung zahlen müssen.

Der wirtschaftliche Erfolg der Zertifizierung kann sich auch über die Verbreitung und Bekanntheit verbessern. So kann das Vorhandensein eines AUDITOR-Zertifikats zukünftig ein Pflichtkriterium bei (öffentlichen) Ausschreibungen werden. Ähnliches wurde bspw. beim BSI C5 im Cloud-Umfeld bereits beobachtet.

Maßgeblich für die Verwertbarkeit ist die erfolgreiche Genehmigung der Zertifizierungskriterien durch die zuständige Datenschutz-Aufsichtsbehörde sowie die Aufnahme des Zertifizierungsprogramm bei der DAkkS. Somit können Zertifizierungsstellen eine Akkreditierung nach AUDITOR beantragen und anschließend die Zertifizierung am Markt anbieten. Zurzeit wird überlegt, ob der Prozess zur

europäischen Anerkennung angestoßen werden soll, sodass AUDITOR in allen EU-Mitgliedsstaaten gültig und anwendbar ist.

2.4.7. Wissenschaftliche Verwertung

Die wissenschaftliche Verwertung der Ergebnisse des Projekts bestand überwiegend in der Veröffentlichung in wissenschaftlichen Publikationen (siehe Kapitel 2.6). Ferner wurden die Ergebnisse des Vorhabens auf einschlägigen wissenschaftlichen, Fachkonferenzen präsentiert. Zudem haben wissenschaftliche Mitarbeiter: innen der Universität Kassel und des KIT Dissertationen zum Thema des Projekts angefertigt. Auch wurden studentische Abschlussarbeiten mit Projektbezug abgeschlossen. Forschungsergebnisse des Projektes sind zudem in die Lehre im Rahmen von Bachelor- und Masterveranstaltungen der Universität Kassel und des KIT eingeflossen.

2.5. Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Während es bereits eine Vielzahl an Zertifizierungen sowie Gütesiegel am Markt zu Projektbeginn gab, erfordert der Geltungsbeginn der Datenschutz-Grundverordnung die Weiterentwicklung dieser bzw. Neuentwicklung von Datenschutzzertifizierungen, denn Art. 42 und 43 DSGVO legen verbindliche Anforderungen fest (insb. die Bewilligung von Zertifizierungsverfahren). Bestehende Gütesiegel, welche die Anforderungen nicht erfüllen, können grundsätzlich durch die DAkkS verboten werden.

Der EDSA führt ein öffentliches Register über genehmigte Zertifizierungskriterien.[7] Die DAkkS listet alle Zertifizierungsprogramme auf, nachdem sich Zertifizierungsstellen akkreditieren können.[8]

In Deutschland konnte lediglich das Siegel der EuroPriSe Cert GmbH vor AUDITOR bewilligt werden. Es ist das EU-weit erste private Unternehmen mit von der zuständigen Aufsichtsbehörde genehmigten Zertifizierungskriterien, deren Datenschutzsiegel speziell für jegliche Art von Auftragsverarbeitung gilt. Im Gegensatz zu AUDITOR umfasst das Siegel einen speziellen Zuschnitt auf das Cloud-Computing also gerade nicht. 2022 vertrat der EDSA die Auffassung, dass die Zertifizierungskriterien mit der Datenschutz-Grundverordnung im Einklang stehen, was dazu führte, dass die Europrivacy-Zertifizierungskriterien sich das Label des allerersten „Europäischen Datenschutzsiegels“ (gemäß Art. 42 Abs. 5 DSGVO) zu eigen machen konnten. Allerdings wird EuroPriSe alleinig durch EuroPriSe Cert GmbH vertrieben, im Gegensatz zu AUDITOR, welches von jeder akkreditierten Zertifizierungsstelle angeboten und durchgeführt werden kann.

Auf europäischer Ebene sind mittlerweile weitere Zertifizierungsverfahren gelistet. Die luxemburgische Datenschutzkommission (Commission nationale pour la protection des données) hat als zuständige Aufsichtsbehörde dem EDSA ihre eigenen, ebenfalls nicht Cloud-Dienst spezifischen, Kriterien (GDPR-CARPA oder Europrivacy-Zertifizierungskriterien) zur Genehmigung vorgelegt und errang damit einen

[7] Siehe https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en
[8] Siehe https://www.dakks.de/de/akkreditierungsfaehige-programme.html

Erfolg auf der Ebene der öffentlich-rechtlichen Zertifizierer. Es wurde am 12.10.2022 zudem als erstes europäisches Datenschutzsiegel anerkannt. Dabei basiert GDPR-CARPA auf internationalen Standards zur Wirtschaftsprüfung. GDPR-CARPA erfüllt jedoch nicht die Anforderungen von den deutschen Datenschutz-Aufsichtsbehörden an eine Datenschutzzertifizierung, welche Zertifizierungen als Konformitätsbewertung gemäß ISO/IEC 17065 festlegen und ergänzende Anforderungen definiert haben. Die Anwendbarkeit und Anerkennung von GDPR-CARPA innerhalb von Deutschland ist daher kritisch zu betrachten.

AUDITOR grenzt sich gegenüber den anderen Zertifizierungsverfahren wie GDPR-CARPA und EuroPriSe maßgeblich durch die Fokussierung auf Cloud-Dienste ab. Während hingegen andere Zertifizierungsverfahren allgemein die Auftragsverarbeitung nach der Datenschutz-Grundverordnung attestierten, berücksichtigt AUDITOR die Spezifika von Cloud-Diensten und auch die Cloud-Anbieter in ihrer Rolle als Verantwortliche zur Bereitstellung der Cloud-Dienste.

Obwohl viele weitere Projekte zur Entwicklung neuer Datenschutzzertifizierungen gestartet wurden (bspw. von ePrivacy GmbH), wurden diese (nach bestem Kenntnisstand) nicht vollendet. Grund hierfür ist der äußerst langwierige, hochkomplexe und aufwendige europäische Bewilligungsprozess für Zertifizierungsverfahren. Es ist daher davon auszugehen, dass AUDITOR als einzige Datenschutzzertifizierung für Cloud-Dienste eine große Marktreichweite haben wird.

Daneben existieren einige genehmigte Verhaltensregeln (Code of Conduct) nach Art. 40 DSGVO. So etwa derjenige der Cloud Security Alliance (CSA). Der CSA-Verhaltenskodex zielt ebenfalls auf die Einhaltung der Datenschutz-Grundverordnung und bietet einen einheitlichen und umfassenden Rahmen für deren Einhaltung. Er ist so konzipiert, dass er sowohl ein Compliance-Tool für die Einhaltung der Datenschutz-Grundverordnung als auch Transparenzrichtlinien für das vom Cloud-Service-Anbieter gebotene Datenschutzniveau bietet. Mit dem Data Protection Code of Conduct for Cloud Infrastructure Service Providers (CISPE) und dem EU Data Protection Code of Conduct for Cloud Service Providers (SCOPE EUCloudCOC), liegen zwischenzeitlich genehmigte Verhaltensregeln vor, welche auch einen Cloud-Fokus aufweisen. SCOPE Europe sieht einen strengeren Überwachungsrahmen der Verhaltensregeln vor. So soll bspw. die Bewertung der Einhaltung Vorgaben auf jährlicher Basis überwacht werden. Die AUDITOR-Zertifizierung geht darüber hinaus und fordert nicht nur die reguläre Überwachung, sondern umfasst insbesondere ein sehr umfassendes initiales Zertifizierungsaudit vor Vergabe des Zertifikats. Ebenso wie ein genehmigtes Zertifizierungsverfahren, kann mit genehmigten Verhaltensregeln die Einhaltung entsprechender Vorgaben nach der Datenschutz-Grundverordnung indiziell nachgewiesen werden. Obgleich er in den einschlägigen DSGVO-Vorschriften in einem Atemzug mit den genehmigten Zertifizierungsverfahren genannt wird, dürfte ihm bei der Frage, ob der Nachweis erbracht ist, geringeres Gewicht zukommen, da er Ausdruck stärkerer (Eigen-)Interessenbindung der beteiligten Akteure ist.

2.6. Veröffentlichungen der Ergebnisse

Das Projekt wurde durch eine fortlaufende wissenschaftliche Begleitforschung unterstützt, welche wichtige und praxis-relevante Erkenntnisse u.a. zur Wirkung von Zertifizierungen auf Kunden, der

Adoption durch Unternehmen, zur Umsetzung von Zertifizierungskriterien in Geschäftsprozessen, sowie aus einer rechtlichen Perspektive zu Datenschutzzertifizierungen hervorbrachte. So hat die Forschung zum Beispiel gezeigt, dass die Übernahme der Zertifizierung in einem reinen Top-Down-Ansatz (d. h. die Verwendung der Zertifizierung als Blaupause für die Ableitung von Organisationspraktiken und Arbeitsanweisungen) die Ist-Situation der Organisation vernachlässigt. Dies hat zur Folge, dass es zu einer oberflächlichen Implementierung der Kriterien oder sogar zu offenem Widerstand von Mitarbeitern kommen kann. Als Abhilfe sollte ein gemischter (sog. "diskursiver") Ansatz gewählt werden, bei dem der Ist-Zustand des Unternehmens berücksichtigt wird und Verbesserungsvorschläge auf Basis der Zertifizierung einbezogen werden können.

Im Rahmen der Öffentlichkeitsarbeit und Dissemination wurden zudem eine Vielzahl an Newsartikeln über AUDITOR veröffentlicht, Vorträge gehalten und Veranstaltungen sowie Messebesuche absolviert (siehe Kapitel 2.1.8).

Im Folgenden werden ausgewählte Publikationen mit direkten Projektbezug (2.6.1) oder zum Forschungsfeld von IT-Zertifizierungen (2.6.2) sowie Newsartikel (2.6.3), Vorträge und Veranstaltungen (2.6.4) gelistet, welche im Rahmen des Projektes erstellt wurden.

2.6.1. Ausgewählte Publikationen mit direkten Projektbezug

(1) Roßnagel, A., Sunyaev, A., Batman, A., Maier, N., Lins, S., & Teigeler, H. (2017). AUDITOR: Neues Forschungsprojekt zur Datenschutzzertifizierung von Cloud-Diensten nach der DS-GVO. ZD-Aktuell.

(2) Roßnagel, A., Sunyaev, A., Batman, A., Lins, S., Maier, N., & Teigeler, H. (2018). AUDITOR-Kriterienkatalog, Entwurfsfassung 0.7, Beitrag zum Forschungsprojekt AUDITOR

(3) Maier, N., & Bile, T. (2019). Die Zertifizierung nach der DSGVO: Innovatives, aber hochkomplexes Instrument. Datenschutz und Datensicherheit, 43(8).

(4) Maier, N., Lins, S., Teigeler, H., Roßnagel, A., & Sunyaev, A. (2019). Die Zertifizierung von Cloud-Diensten nach der DSGVO. Datenschutz und Datensicherheit-DuD, 43(4).

(5) Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR-Kriterienkatalog – Entwurfsfassung 0.9 (deutsche Fassung/englische Fassung).

(6) Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR-Kriterienkatalog – Entwurfsfassung 0.99 (deutsche Fassung/englische Fassung).

(7) Maier, N. (2019). Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“. ZD-Aktuell.

(8) Maier, N., Lins, S., Teigeler, H., Roßnagel, A., Sunyaev, A. (2020). AUDITOR: Einreichung des Zertifizierungsprogramms bei der deutschen Akkreditierungsstelle. ZD-Aktuell 2020.

(9) Maier, N., Pawlowska, I. M., Lins, S., & Sunyaev, A. (2020). Die Zertifizierung nach der DS-GVO. Transparenz und Vertrauen für Nutzer digitaler Dienste? Zeitschrift für Datenschutz ZD, (9).

(10) Maier-Reinhardt, N. (2021). Vergleich nationaler Akkreditierungsanforderungen nach Art. 43 Abs. 3 i.V.m. 57 Abs. 1 lit. p DS-GVO. ZD-Aktuell.

(11) Maier-Reinhardt, N. (2021). Nationale Akkreditierungsanforderungen nach Art. 43 Abs. 3 DSGVO iVm Art. 57 Abs. 1 lit. p DS-GVO – Vergleich Dänemark und Niederlande. ZD-Aktuell.

(12) Müller, J. (2022). AUDITOR: Zwischenstand im Forschungsprojekt „European Cloud Service Data Protection Certification“. ZD-Aktuell.

2.6.2. Ausgewählte Publikationen mit Bezug zum Forschungsfeld der IT-Zertifizierung

(13) Lins, S., & Sunyaev, A. (2017). Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness. Proceedings of the International Conference on Information Systems (ICIS).

(14) Lins, S., Schneider, S., & Sunyaev, A. (2019). Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services. 2. Auflage, Springer Gabler Berlin, Heidelberg.

(15) Lansing, J., Benlian, A., & Sunyaev, A. (2018). “Unblackboxing” decision makers’ interpretations of IS certifications in the context of cloud service certifications. Journal of the Association for Information Systems, 19 (11).

(16) Lansing, J., Siegfried, N., Sunyaev, A., & Benlian, A. (2019). Strategic signaling through cloud service certifications: Comparing the relative importance of certifications’ assurances to companies and consumers. The Journal of Strategic Information Systems, 28(4).

(17) Adam, M., Niehage, L., Lins, S., Benlian, A., & Sunyaev, A. (2020). Stumbling over the trust tipping point–The effectiveness of web seals at different levels of website trustworthiness. Proceedings of the 28th European Conference on Information Systems (ECIS).

(18) Greulich, M., Lins, S., & Sunyaev, A. (2020). Toward Uncovering Patterns of Certification Internalization. Proceedings of the International Conference on Information Systems (ICIS).

(19) Renner, M., Lins, S., & Sunyaev, A. (2021). A taxonomy of IS certification's characteristics. Proceedings of the 2021 2nd International Conference on Internet and E-Business.

(20) Löbbers, J., Lins, S., Kromat, T., Benlian, A., & Sunyaev, A. (2022). A multi-perspective lens on web assurance seals: contrasting vendors’ intended and consumers’ perceived effects. Electronic Commerce Research.

(21) Danylak, P., Lins, S., Hsu, C., & Sunyaev, A. (2022). Making sense of certification internalization: A process model for implementing information security and data protection certifications. Workshop on Information Security and Privacy.

(22) Danylak, P., Brecker, K., Lins, S., & Sunyaev, A. (2022). Certifications to Safeguard data protection standards? How superficial internalization thwarts the plan. Forum Privatheit.

(23) Lins, S., Kromat, T., Löbbers, J., Benlian, A., & Sunyaev, A. (2022). Why don't you join in? A typology of information system certification adopters. Decision Sciences, 53(3).

(24) Danylak, P., Lins, S., Greulich, M., & Sunyaev, A. (2022). Toward a unified framework for information systems certification internalization. Proceedings of the 2022 IEEE 24th Conference on Business Informatics (CBI).

(25) Lins, S., & Sunyaev, A. (2023). Advancing the presentation of IS certifications: theory-driven guidelines for designing peripheral cues to increase users' trust perceptions. Behaviour & Information Technology, 42(13).

(26) Lins, S., Becker, J. M., Lyytinen, K., & Sunyaev, A. (2023). A design theory for certification presentations. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 54(3).

(27) Adam, M., Lins, S., Sunyaev, A., & Benlian, A. (2024). The contingent effects of is certifications on the trustworthiness of websites. Journal of the Association for Information Systems, 25(3).

(28) Lins, S., Greulich, M., Löbbers, J., Benlian, A., & Sunyaev, A. (2024). Why so skeptical? Investigating the emergence and consequences of consumer skepticism toward web seals. Information & Management, 61(2).

2.6.3. Ausgewählte Newsartikel zu AUDITOR

(1) 06.12.17 Forschungsprojekt Auditor: Zertifizierung für die Datenschutz-Cloud. https://www.heise.de/news/Forschungsprojekt-Auditor-Zertifizierung-fuer-die-Datenschutz-Cloud-3911096.html

(2) 15.12.17 „AUDITOR" will Cloud-Dienste europaweit zertifizieren. https://www.cloudcomputing-insider.de/auditor-will-cloud-dienste-europaweit-zertifizieren-a-669750/

(3) 21.03.18. Forschungsprojekt Auditor: Im Dschungel der Wolken. https://www.connect-professional.de/datacenter-verkabelung/im-dschungel-der-wolken.151830.html

(4) 27.04.18. Innovations Report: Datenschutz: Cloud-Dienste europaweit zertifizieren. https://www.innovations-report.de/fachgebiete/informationstechnologie/datenschutz-cloud-dienste-europaweit-zertifizieren/

(5) 27.04.18. Informationsdienst Wissenschaft: Datenschutz: Cloud-Dienste europaweit zertifizieren. https://idw-online.de/de/news693391

(6) 30.04.18. Plattform für Prozess-, Qualitäts-, Risikomanagement und Technische Dokumentation: Datenschutz: Cloud-Dienste europaweit zertifizieren. https://www.pqrm.at/2018/04/30/datenschutz-cloud-dienste-europaweit-zertifizieren/

(7) 22.05.18. Umbau in der Wolke: Mit der EU-DSGVO Transparenz und Sicherheit in der Cloud-Branche schaffen. https://www.informatik-aktuell.de/betrieb/virtualisierung/mit-der-eu-dsgvo-transparenz-und-sicherheit-in-der-cloud-branche-schaffen.html

(8) 29.05.18. AUDITOR: Cloud-Dienste europaweit datenschutzkonform zertifizieren. https://www.cloud-computing-report.de/auditor-cloud-dienste-europaweit-datenschutzkonform-zertifizieren/29-05-2018/

(9) 03.06.18. Cloud-Security: zertifiziert statt nebulös. https://www.kes.info/aktuelles/kes/cebit2018/

(10) 06.06.18. Staatssekretär Nussbaum: BMWi-Projekt AUDITOR stellt datenschutzkonforme Cloud-Dienste sicher.

https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2018/20180606-nussbaum-bmwi-projekt-auditor-stellt-datenschutzkonforme-cloud-dienste-sicher.html

(11) 07.06.18. Radio Beitrag - Campus Report: TÜV-Plakette für Cloud-Dienste. https://soundcloud.com/karlsruherinstitutfuertechnologie/campus-report-tuv-plakette-fur-cloud-dienste

(12) 08.06.18. Mit AUDITOR in die Cloud. https://www.move-online.de/meldung_29110_Mit+AUDITOR+in+die+Cloud.html

(13) 08.06.18. BMWi-Projekt AUDITOR stellt datenschutzkonforme Cloud-Dienste sicher. http://www.beraternews.net/it/datensicherheit/bmwi-projekt-auditor-stellt-datenschutzkonforme-cloud-dienste-sicher-35714014/

(14) 12.06.18. Cloud-Computing / DSGVO - Das Thema Datenschutz. https://www.computer-automation.de/unternehmensebene/produktionssoftware/artikel/154260/

(15) 15.06.18. Die CEBIT 2018 verordnet sich Coolness. https://www.cloudcomputing-insider.de/die-cebit-2018-verordnet-sich-coolness-a-724792/

(16) 15.06.18. AUDITOR: Kriterien für Cloud-Zertifizierung vorgestellt. https://www.behoerden-spiegel.de/2018/06/15/auditor-kriterien-fuer-cloud-zertifizierung-vorgestellt-2/

(17) 12.06.18. Das Thema Datenschutz. https://www.security-insider.de/Datenschutzzertifizierung-von-cloud-diensten-a-750529/

(18) 21.09.18. Datenschutzzertifizierung von Cloud-Diensten. 21.09.18. Datenschutzzertifizierung von Cloud-Diensten

(19) 23.11.2018. Gemischte Bilanz nach sechs Monaten DSGVO. https://www.eco.de/presse/gemischte-bilanz-nach-sechs-monaten-dsgvo/

(20) 23.11.2018. DSGVO: Mehr Klarheit und Rechtssicherheit gewünscht. https://www.marketing-boerse.de/News/details/1847-DSGVO/151981

(21) 03.01.2019. DSGVO ist zugleich Risiko und Chance. https://www.security-insider.de/dsgvo-ist-zugleich-risiko-und-chance-a-784379/

(22) 02.04.2019. DSGVO: Die zertifizierte Cloud kommt! https://blog.direkt-gruppe.de/dsgvo-die-zertifizierte-cloud-kommt/

(23) 03.04.2019. EU-weite Datenschutzzertifizierung von Cloud-Diensten. https://www.security-insider.de/eu-weite-Datenschutzzertifizierung-von-cloud-diensteneu-weite-Datenschutzzertifizierung-von-cloud-diensten-rueckt-naeher-a-815673/

(24) 03.04.2019. Prüfstandard für Datenschutzzertifizierung von Cloud-Diensten. https://www.funkschau.de/telekommunikation/artikel/164080/

(25) 26.04.2019. EuroCloud: Datenschutz aus der Wolke ist Trumpf. https://www.eco.de/presse/eurocloud-datenschutz-aus-der-wolke-ist-trumpf/

(26) 29.04.2019. Initiativen zur Standardisierung industrieller Cloud-Angebote. Smart Factory und die nahtlose Kommunikation, https://www.cloudcomputing-insider.de/smart-factory-und-die-nahtlose-kommunikation-a-823477/

(27) 07.06.2019. DSGVO-Zertifizierung für Cloud Provider. https://www.computerwoche.de/a/dsgvo-zertifizierung-fuer-cloud-provider,3547161

(28) 12.11.2019. solutionsHUB: Cloud, Data, Security. https://blog.direkt-gruppe.de/nachbericht-solutionshub/

(29) 02.12.2019. Vertrauen ist gut, Kontrolle ist besser. https://www.it-daily.net/it-management/cloud-computing/22923-vertrauen-ist-gut-kontrolle-ist-besser

(30) 13.12.2019. „AUDITOR“ wird zum europäischen Datenschutz Gütesiegel weiterentwickelt. http://www.imittelstand.de/themen/presse.html?boxid=986036

(31) 20.03.2020. Innovative Certification for GDPR Compliance of Cloud Services. https://www.dotmagazine.online/issues/cloud-and-orientation/gdpr-compliance-of-cloud-services@next-issue-gigex

2.6.4. Ausgewählte Vorträge und Veranstaltungen

(1) Am 08.11.2017 organisierte das KIT gemeinsam mit der Universität Kassel das Projektkickoff in Kassel. Dort wurden Projektpartner und assoziierte Partner eingeladen und gemeinsam die Projekt-Road-Map diskutiert.

(2) Am 16.11.2017 hielt das Konsortium ein Webinar bei Fabasoft zur Zertifizierung von Cloud-Diensten nach der Datenschutz-Grundverordnung.

(3) Uni Kassel mit EuroCloud, eco Verband der Internetwirtschaft, TÜV-Informationstechnik, und Kompetenznetzwerk Trusted Cloud stellten AUDITOR auf der Cloud Security Expo am 29.11.2017 vor. Panel und Dialog zum Thema „EU DSGVO – Wie werden die Verantwortlichkeiten zur Einhaltung des Datenschutzes zwischen Nutzer und Cloud Anbieter geregelt?”.

(4) Vortrag von Prof. Roßnagel der Universität Kassel zum Thema „Datenschutz-Grundverordnung – Herausforderung und Chance für Anbieter und Nutzer“, Trusted Cloud Lounge zu Gast im Bundesministerium für Wirtschaft und Energie am 17.1.2018 in Berlin.

(5) Am 13.03.2018 fand das CloudFest in Rust statt, welches ein wichtiges Forum zum Austausch von Cloud-Service-Anbietern und –Kunden darstellt. Das Konsortium hat an dem CloudFest teilgenommen und Werbung für AUDITOR gemacht.

(6) Vortrag von der Universität Kassel zum Thema „Rechtliche Aspekte des Cloud Computing“ bei der IT-Fachtagung des Deutschen Studentenwerks e.V. am 16. Mai 2018 in Göttingen.

(7) Am 29.05.2018 hat das Konsortium ein Webinar zum Thema EU-DSGVO in Gütesiegeln und Zertifizierungen im Rahmen der Webinar Reihe von Trusted Cloud durchgeführt.

(8) Am 06.06.2018 fand die Projektpräsentation in Berlin statt. Dort wurde der Kriterienkatalog der Fassung 0.7 der Öffentlichkeit präsentiert.

(9) Vortrag von der Universität Kassel zum Thema „Europäische Datenschutzzertifizierung von Cloud-Diensten – Projektvorstellung AUDITOR“ auf der Akkreditierungskonferenz 2018 der DAkkS am 16.6.2018 in Berlin.

(10) Vom 11.06.2018 bis zum 15.06.2018 fand die CEBIT in Hannover statt. Das Projekt AUDITOR hatte einen eigenen Messestand vor Ort und konnte große Aufmerksamkeit erzeugen. Gemeinsam mit der Universität Kassel warb das KIT für AUDITOR, wodurch viele interessante Kontakt geknüpft und sogar neue Assoziierte Partner gewonnen wurden.

(11) 1. Workshop für Cloud Service Provider am 12.7.2018 in Köln, Veranstalter: AUDITOR-Konsortium und EuroCloud Deutschland. Besprechung des Kriterienkatalogs und des Zertifizierungsverfahrens.

(12) AUDITOR-Workshop mit der DAkkS am 29.8.2018 in Kassel.

(13) Das Konsortium nahm am 21.09.2018 bei einer Paneldiskussion auf den Internet Security Days in Brühl teil.

(14) Das Konsortium hat am 11.10.2018 - 12.10.2018 im Schmalenbach Arbeitskreis in Karlsruhe das Projekt AUDITOR vorgestellt.

(15) Am 23.10.2018 wurde ein einzigartiger Workshop mit Vertretern der EU-Kommission DG Justice und DG Connect in Brüssel gemeinsam mit TrustedCloud, der Universität Kassel, dem KIT und dem BMWi durchgeführt. Das Konsortium hat auf diesem Workshop das Projekt AUDITOR vorgestellt, Ergebnisse gemeinsam diskutiert und eine zukünftige gemeinsame Abstimmung mit der EU-Kommission beschlossen.

(16) Vom 07.11.2018 bis zum 08.11.2018 hat das Konsortium auf der TECHWEEK in Frankfurt einen Ausstellerstand auf dem Gemeinschaftstand von eco EuroCloud geleitet und eine Panel-Diskussion geführt. Auf der Messe konnte eine hohe Awareness für das Projekt erreicht werden.

(17) Durchführung des 2. Workshop für Cloud Service Provider vom 15.11.2018 in Berlin. Besprechung des Kriterienkatalogs und des Zertifizierungsverfahrens.

(18) Am 29.11.2018 hat das Konsortium an einer öffentlichen Informationsveranstaltung zur Akkreditierung von Datenschutzzertifizierungen der DAkkS in Berlin teilgenommen, um sich über alle aktuellen Entwicklungen und Anforderungen zu informieren. Zudem wurde das AUDITOR-Projekt als Referenzbeispiel für eine Datenschutzzertifizierung durch das KIT und der DAkkS vorgestellt.

(19) Kick-Off-Veranstaltung am 22.2.2019 in Köln zur Erarbeitung einer DIN SPEC auf Basis des AUDITOR-Kriterienkatalogs (DIN SPEC 27557).

(20) Am 28. März 2019 wurde ein exklusives Treffen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Ulrich Kelber und Vertretern des BfDI in Bonn durchgeführt. Das BfDI hat dem AUDITOR Projektteam unter anderem die Unterstützung auf internationaler Ebene zugesichert.

(21) Am 11. April 2019 hat das Konsortium einen europäischen Workshop zu AUDITOR organisiert und geleitet. Am Workshop haben 30 Teilnehmer aus verschiedensten Institutionen (insb. Datenschutz-Aufsichtsbehörden und Akkreditierungsstellen) und Ländern (bspw. Spanien, Italien, Griechenland, Frankreich, Norwegen, Bulgarien, usw.) teilgenommen. Der Workshop war ein voller Erfolg, denn alle Teilnehmer haben den Mehrwert und den Reifegrad von AUDITOR positiv bewertet.

(22) Am 14. und 15. Mai 2019 veranstaltete das Bundesministerium für Wirtschaft und Energie in Berlin die “Tage der digitalen Technologien”. Auf der Veranstaltung in den Bolle Festsälen hat das Konsortium mit einem eigenen Informationsstand interessierte Besucher über die

aktuellen Fortschritte im Forschungsprojekt informiert und weitere interessante Kontakte aus Forschung und Wirtschaft knüpfen können.

(23) Am 17. Juni 2019 stellte das AUDITOR-Konsortium das Projekt bei Frau Block als Landesbeauftragte für den Datenschutz und Informationsfreiheit (LDI) Nordrhein-Westfalen in Düsseldorf vor. Hierbei wurden nicht nur die wichtigsten Eckdaten des Projektes vorgestellt, sondern vor allem auch die Anforderungen und Prozesse für die Einreichung eines nationalen und anschließend eines europäischen Gütesiegels für den Datenschutz besprochen. Das LDI NRW hat dem Konsortium seine Unterstützung im Rahmen der Programmprüfung zugesichert.

(24) Vom 22. bis zum 27. September 2019 besuchte eine siebzehnköpfige Delegation unter Leitung des BMWi und des Forum Digitale Technologien (FDT) vier spannende Städte an der kanadischen Ostküste. Das Projekt AUDITOR wurde vom KIT im Rahmen der Kanada Roadshow vorgestellt und erfuhr großes Interesse seitens der kanadischen Vertreter.

(25) Gemeinsam mit der Universität Kassel hat das KIT am 21. Oktober 2019 das AUDITOR-Projekt beim Roundtable der Interessengemeinschaft Public Cloud in Mannheim vorgestellt. Ziel des Workshops war unter anderem die Anerkennung von AUDITOR als Best-Practice-Zertifizierung bei der Verarbeitung von personenbezogenen Daten in der Versicherungsbranche.

(26) AUDITOR bei dem Arbeitstreffen der „Deutsch-Chinesischen Arbeitsgruppe Akkreditierung und Konformitätsbewertung“ am 4.11.2019 in Peking.

(27) Das Konsortium hat am 21. und 22. November 2019 im Rahmen des deutsch-österreichischen Austausch an der Veranstaltung „Entwicklung digitaler Technologien - Sichere Cloud Lösungen“ teilgenommen und AUDITOR präsentiert.

(28) Um AUDITOR zu bewerben und Awareness im Markt zu schaffen hat das Konsortium AUDITOR auf dem Experten-Roundtable „Future Cloud 2020“ am 05.02.2020 in Frankfurt vorgestellt.

(29) AUDITOR-Vorstellung beim de.NBI Cloud (Deutsches Netzwerk für Bioinformatik-Infrastruktur) als Websession am 20. Mai 2020.

(30) Präsentation des Projekts AUDITOR (European Cloud Service Data Protection Certification) am 15.6.2020 vor Vertretern internationaler und europäischer Akkreditierungs- und Datenschutz-Aufsichtsbehörden sowie Zertifizierungsstellen und Cloud-Anbietern im Rahmen der Web-Session: „Discussion on how to amend the criteria catalogue to include national requirements of EU member states“.

(31) Das Konsortium hat am 17.02.2021 AUDITOR im Rahmen des GAIA-X Technical Deep Dives vorgestellt. Dabei wurde neben einer kurzen Einführung zum Projekt auch die Zusammenarbeit mit GAIA-X dargestellt.

(32) Das Konsortium hat AUDITOR am 16.04.2021 beim Bundesinstitut für Arzneimittel und Medizinprodukte in der Abteilung „Digitale Gesundheitsanwendungen“ vorgestellt. Die Arbeitsgruppe plante ebenfalls die Entwicklung einer Datenschutzzertifizierung.

(33) Das Konsortium hat AUDITOR am 16.04.2021 im Rahmen des Webinars „Datenschutz am Mittag – Zertifizierung von Cloud-Diensten“ der Stiftung Datenschutz vorgestellt.

(34) Das Konsortium hat AUDITOR auf den Community Days „Governance, Risk, Compliance in der IT“ am 26.04.2021 vorgestellt.

(35) Das Konsortium hat AUDITOR auf den Open Source Automation Days (OSAD) 2022 in München vorgestellt.

(36) Das Konsortium hat AUDITOR auf der Cloud Expo Europe 2022 in Frankfurt an zwei Tagen vorgestellt. Das AUDITOR Konsortium konnte mit einem eigenen Informationsstand interessierte Besucher über die aktuellen Fortschritte im Forschungsprojekt informieren. Somit konnten weitere interessante Kontakte aus Forschung und Wirtschaft geknüpft werden.

3. Fazit und Ausblick

Mit der Geltung der Datenschutz-Grundverordnung wurden neue Anforderungen an die Datenschutzzertifizierung gestellt. Gleichzeitig haben Art. 42 und 43 DSGVO den Grundstein für die datenschutzrechtliche Zertifizierung gelegt. Durch Zertifizierungen können Cloud-Anbieter nachweisen, dass ihre Datenverarbeitungsvorgänge im Einklang mit den Anforderungen der Grundverordnung stehen. Damit können Zertifizierungen zur Transparenz und zur Vertrauensbildung im Cloud-Dienst-Markt beitragen. Das Forschungsprojekt AUDITOR wurde gefördert, um eine nachhaltig anwendbare EU-weite Datenschutzzertifizierung zu entwickeln, umzusetzen und zu erproben. AUDITOR hilft insbesondere KMU bekannte Probleme zu adressieren, Transparenz zu schaffen und bei der Auftragsverarbeitung Rechtssicherheit auf einer europäischen Ebene zu vermitteln.

Um eine nachhaltige Datenschutzzertifizierung zu konzipieren, wurde zunächst ein Kriterienkatalog entwickelt und eine entsprechende Standardisierung als DIN SPEC initiiert. Außerdem wurde ein geeignetes Zertifizierungsverfahren zur Durchführung einer anerkannten Datenschutzzertifizierung konzipiert und in einem KBP für die Akkreditierung formuliert. Das entwickelte Zertifizierungsverfahren wurde in drei Pilotierungen bei Cloud-Anbietern erprobt und validiert. Das Zertifizierungsverfahren hat anschließend den formalen und sehr aufwendigen Bewilligungsprozess erfolgreich durchlaufen. Das AUDITOR-Projekt hat somit erfolgreich die erste Datenschutzzertifizierung innerhalb von Europa geschaffen.

Gemäß Art. 42 Abs. 5 DSGVO können Zertifizierungskriterien, die durch den EDSA im Rahmen des Kohärenzverfahrens nach Art. 64f. DSGVO genehmigt worden sind, „zu einer gemeinsamen Zertifizierung, dem europäischen Datenschutzsiegel, führen“. Die Etablierung eines solchen Siegels wirkt der Fragmentierung im Bereich der Datenschutzzertifizierung entgegen und trägt zur Harmonisierung bei. Da die europaweite Zertifizierung gerade für das Cloud Computing aufgrund des länderübergreifenden Cloud-Dienst-Marktes große Vorteile verspricht, strebt AUDITOR künftig die europaweite Anerkennung als cloud-spezifischer Zertifizierungsmechanismus an.

Das AUDITOR-Konsortium dankt dem Bundesministerium für Wirtschaft und Klimaschutz für die Projektförderung und fortlaufende Unterstützung. Ebenfalls danken wir dem Projektträger DLR für die langjährige Unterstützung und Befürwortung des Projektes.

Das AUDITOR-Projekt ist dankbar für die fortlaufende und ehrenamtliche Mitwirkung vieler assoziierter Partner des Projektes, darunter insb. dem Kompetenznetzwerk TrustedCloud e.V., der Hornetsecurity GmbH und dem VOICE-Bundesverband der IT-Anwender e.V.