Forschungsprojekt AUDITOR

European Cloud Service Data Protection Certification

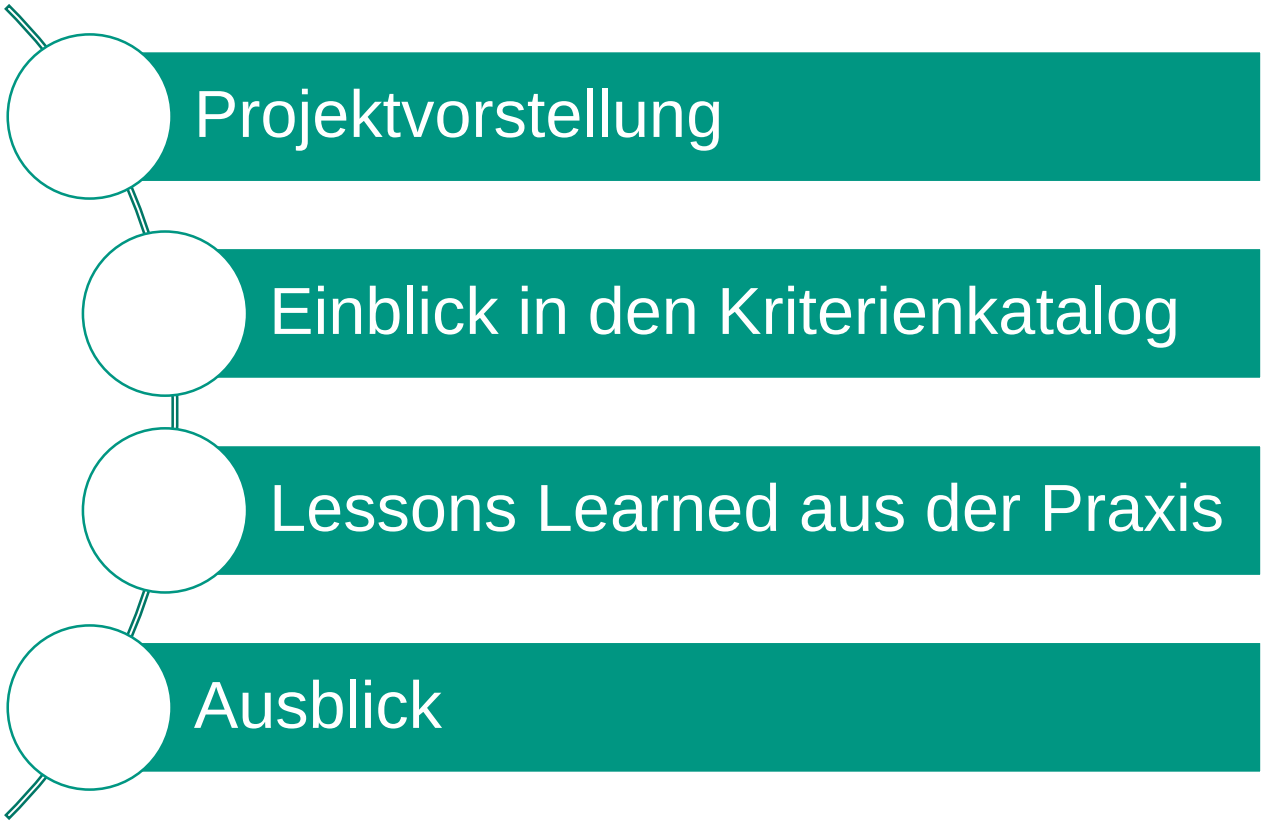
Datenschutz am Mittag „Zertifizierung von Cloud-Diensten“
16.04.2021

Dr. Natalie Maier-Reinhardt, Universität Kassel
Kai Osterhage, datenschutz cert
Sebastian Lins, Karlsruher Institut für Technologie

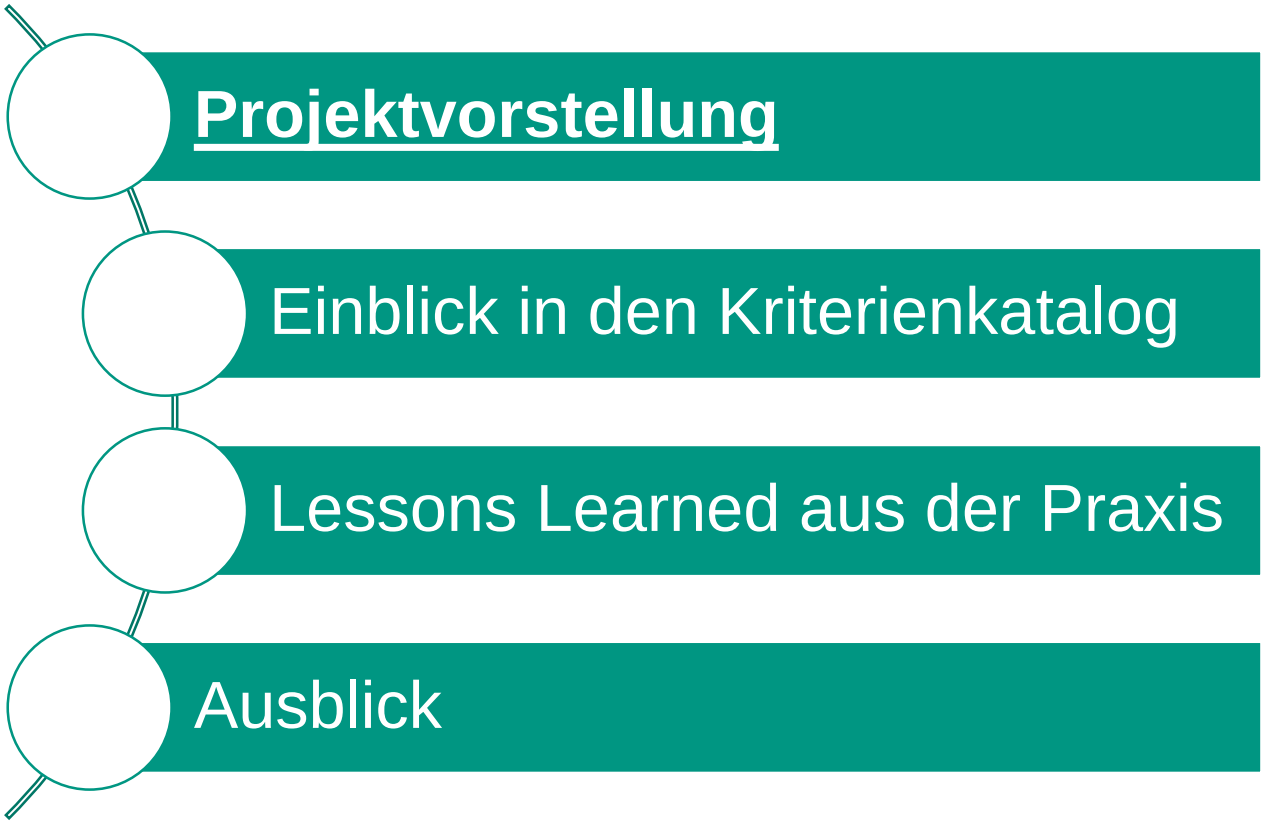
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Kurzvorstellung der Referendierenden

Agenda


Projektvorstellung
Einblick in den Kriterienkatalog
Lessons Learned aus der Praxis
Ausblick

Agenda


Projektvorstellung
Einblick in den Kriterienkatalog
Lessons Learned aus der Praxis
Ausblick

Konformität mit DSGVO ist Top-Kriterium bei der Anbieterauswahl

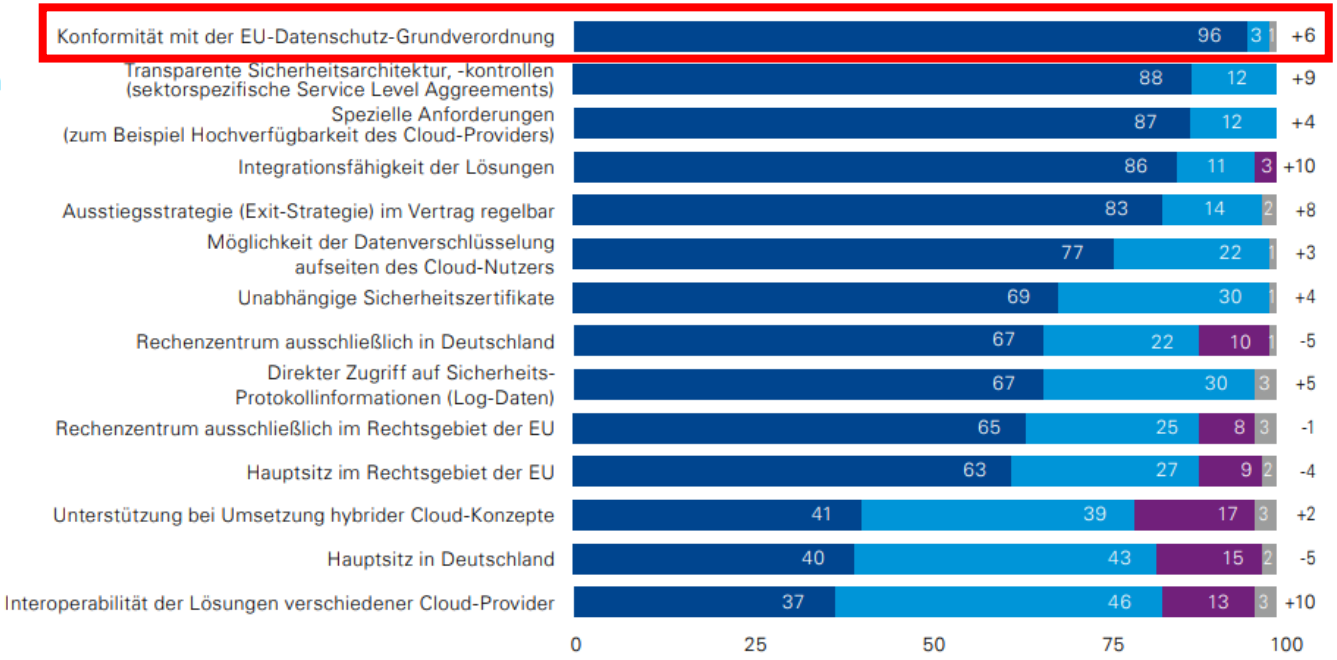
KPMG Cloud-Monitor 2020

Anforderungen an Cloud-Anbieter

Wie wichtig sind die folgenden Kriterien und Leistungen bei der Auswahl eines Cloud-Providers für Ihr Unternehmen?

Anteil (gewichtet) in Prozent der Unternehmen, die Cloud-Lösungen nutzen, planen oder diskutieren, n = 533/521

Von 100 abweichende Werte ergeben sich aus Rundungsdifferenzen.



Quelle: KPMG in Deutschland, 2020

Die Konformität mit der DSGVO ist Auswahlkriterium Nummer 1

Dschungel der (Cloud-Service-)Zertifizierungen

auditor

Bereits heutzutage besteht ein Dschungel an Zertifizierungen und Standards

Trusted Cloud

EuroCloud StarAudit

C5 Cloud Computing Compliance Controls Catalogue

Trusted Cloud
Pilotprojekt Datenschutz-Zertifizierung für Cloud-Dienste

TÜVRheinland ZERTIFIZIERT
Certified Cloud Service
www.tuv.com
ID 0000043141

BSI IT-Grundschutz

CSA cloud security alliance®

International Organization for Standardization ISO 27017:2015

EuroPriSe European Privacy Seal

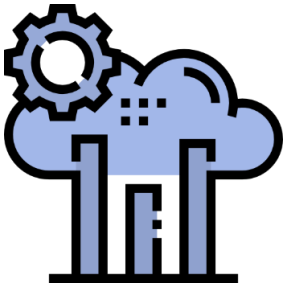
u.v.m.

Quelle: Neubauer, C., Weiss, A., Lins, S., & Sunyaev, A. (2018). *Vergleich existierender Zertifizierungen zum Nachweis vertrauenswürdiger Cloud-Services*. In H. Krcmar, C. Eckert, A. Roßnagel, A. Sunyaev, & M. Wiesche (Eds.), Management sicherer Cloud-Services (pp. 81–90). Springer Fachmedien Wiesbaden.

Neue Herausforderungen durch die EU DSGVO

Art. 42 – EU-DSGVO – Zertifizierung

1. 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. Den besonderen **Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen** wird Rechnung getragen.



Den **Zertifizierungs-gegenstand** bilden **Verarbeitungsvorgänge** von personenbezogenen Daten

Genehmigung der Kriterienkataloge durch EU-Ausschuss und nationalen Aufsichtsbehörden

Akkreditierungspflicht gemäß Art. 43 Abs. 1 DSGVO: **Die Mitgliedstaaten stellen sicher, dass Zertifizierungsstellen akkreditiert werden**

AUDITOR
European Cloud Service Data Protection Certification

- Nachfolgeprojekt des Trusted Cloud Datenschutz-Profils für Cloud-Dienste (TCDP) (tcdp.de)
- Förderung durch das Bundesministerium für Wirtschaft und Energie
- November 2017 – Oktober 2021 (vor.)
- Gesamtvolumen: >3,4 Mio. Euro

- Ziel des Forschungsprojekts AUDITOR ist die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutz-Zertifizierung von Cloud-Diensten

Weitere Informationen unter
www.auditor-cert.de

Verbundkoordinator:

Karlsruher Institut für Technologie

Kooperationspartner:

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Die Praxispartner im Projekt AUDITOR stellen eine praxisnahe Forschung und Verwertung der Ergebnisse sicher

auditor

Feld- und Transferpartner mit Unterauftrag

Trusted Cloud

HORNETSECURITY®

VOICE Bundesverband der IT-Anwender e.V.

Feld- und Transferpartner

Microsoft

SAP

FUJITSU

salesforce

IBM

Propstack

Consultix

CRM!ADDON

1&1 IONOS

MGID

pwc

xworks.365 TRUSTED COLLABORATION

TechGDPR

Bundesamt für Sicherheit in der Informationstechnik

MKM + PARTNER RECHTSANWÄLTE

T..

direktgruppe

TACTICX

TÜVRheinland® Genau. Richtig.

SCOPE EUROPE

TÜV SÜD Management Service

TÜViT® TÜV NORD GROUP

UNiSCON Sealed Cloud Technologies A member of TÜV SÜD

SMART SERVICE POWER VIVAI

CAS SOFTWARE

WALLSEC

ePrivacy

Fabasoft

x-ion GmbH

Ziele und bisherige Projektergebnisse

Entwicklung einer nachhaltigen, anwendbaren Datenschutz-Zertifizierung

auditor

Kriterienkatalog

- Kriterienkatalog für die Zertifizierung von Cloud-Diensten nach der DSGVO
- Modularität
- Berücksichtigung bestehender Standards und Kriterienwerke, insb. ISO 27001

→ AUDITOR-Kriterienkatalog

Anwendbarkeit

- Organisations-strukturen
- Methoden
- Verfahren

zur Durchführung einer europaweit anerkannten Datenschutz-Zertifizierung

→ AUDITOR-Konformitätsbewer-tungsprogramm

Nachhaltigkeit

- Geschäftsmodelle
- Rahmen-bedingungen
- Gestaltungs-empfehlungen
- Standardisierung

für ein nachhaltig erfolgreiches AUDITOR-Verfahren

→ Konzept zur Weiterführung, DIN-SPEC

Pilotierung

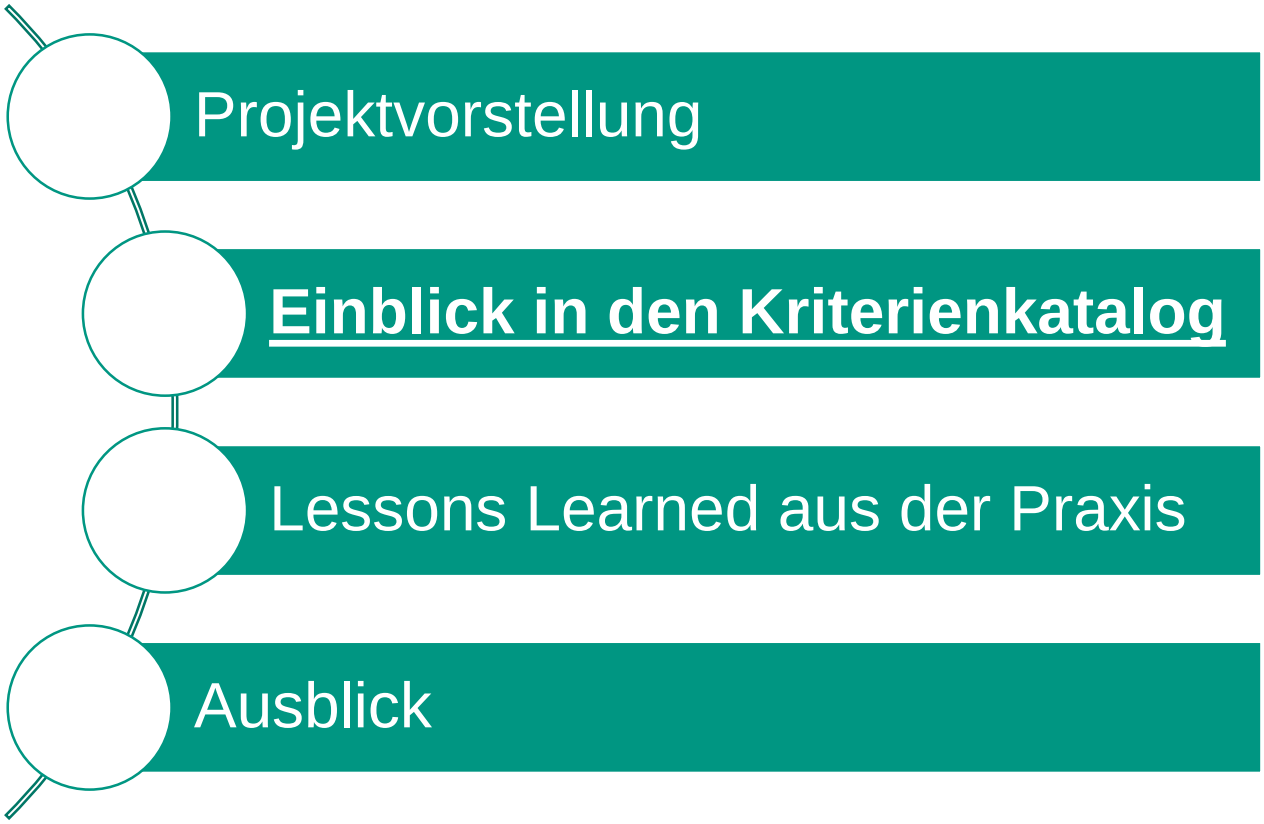
Ganzheitliche

- Erprobung,
- Evaluierung und
- Validierung

in drei Use-Cases mit Praktikern

→ Pilot-Zertifizierungen (nicht akkreditiert)

Agenda


Projektvorstellung
Einblick in den Kriterienkatalog
Lessons Learned aus der Praxis
Ausblick

AUDITOR-KRITERIENKATALOG

AUDITOR-Kriterienkatalog – Aufbau

AUDITOR-Kriterienkatalog

Kriterium
[..]

Erläuterung
[..]

Umsetzungshinweise
[..]

Nachweise
[..]

Normative Anforderungen der DSGVO an Cloud-Anbieter.

Die Erfüllung ist notwendig für den Erhalt des Zertifikats

Unverbindliche Hinweise auf rechtliche Grundlagen und Zielsetzungen.

Sollen das Verständnis der Kriterien erleichtern

Unverbindliche techn.-org. Hinweise, wie der Cloud-Anbieter die Kriterien erfüllen kann.

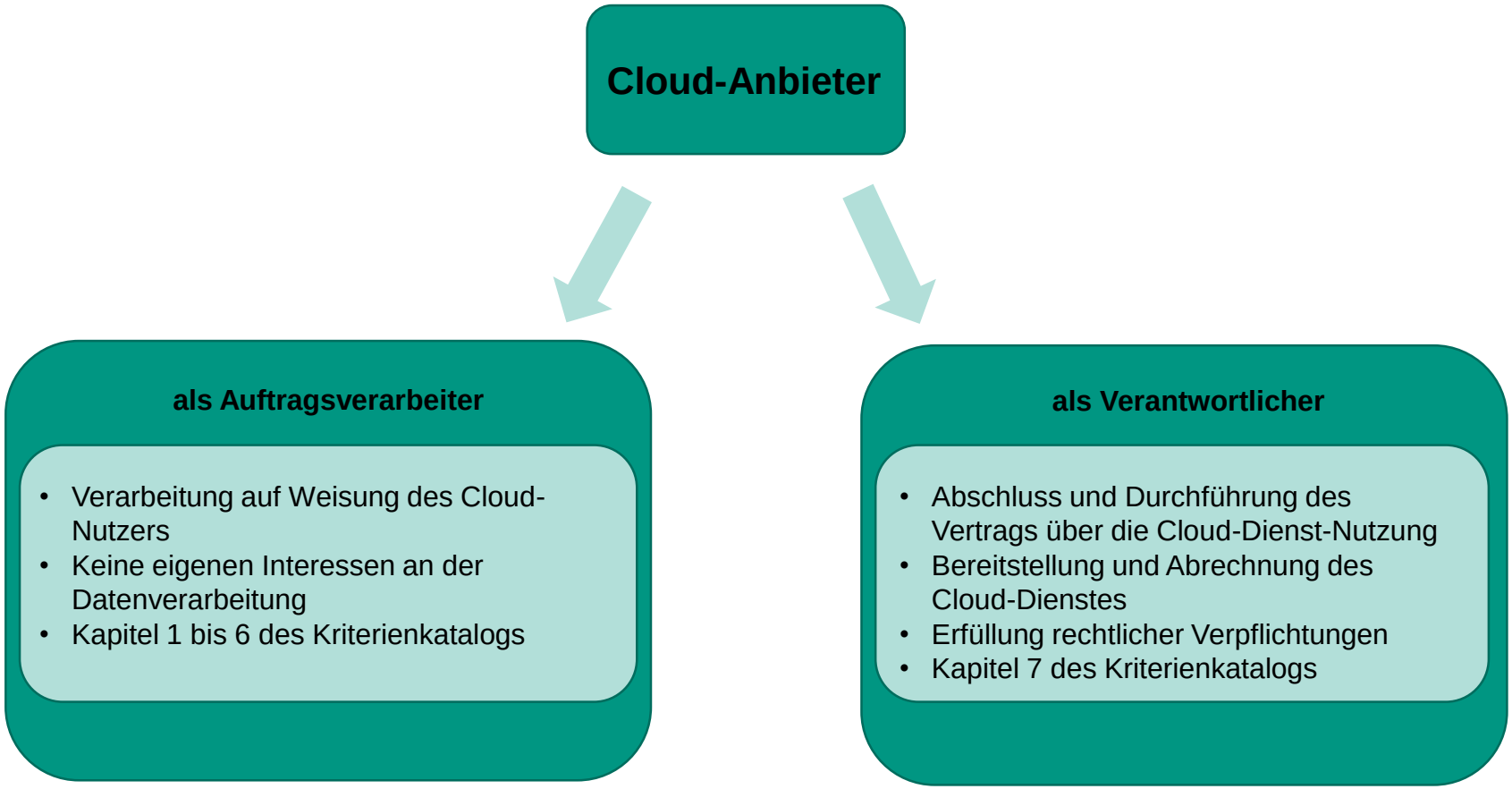
Exemplarische Leitlinien und Hilfestellungen

Verweise auf Standards wie ISO/IEC 27001/2, 27018, 27701, BSI C5 etc.

Unverbindliche Hinweise, wie der Cloud-Anbieter die Erfüllung des Kriteriums nachweisen kann.

Sollen bei der Beurteilung der Einhaltung der Kriterien unterstützen

AUDITOR-Kriterienkatalog – Rollen des Cloud-Anbieters



AUDITOR-Kriterienkatalog – Themen

- Kapitel 1: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung
  - 8 Kriterien zu Abschluss, Form und Inhalten der Vereinbarung
- Kapitel 2: Rechte und Pflichten des Cloud-Anbieters
  - 11 Kriterien zur Datensicherheit nach drei Schutzklassen
  - 2 Kriterien zu Weisungen, 7 zu Betroffenenrechten, 3 zu weiteren Pflichten
- Kapitel 3: Datenschutz-Managementsystem des Cloud-Anbieters
  - 6 Kriterien zu Managementpflichten

Ziel: Nachweis der Vereinbarkeit von Verarbeitungsvorgängen mit den Regelungen der DSGVO

AUDITOR-Kriterienkatalog – Themen

- Kapitel 4: Datenschutz durch Systemgestaltung
  - 2 Kriterien zur Technikgestaltung und zu Voreinstellungen
- Kapitel 5: Subauftragsverarbeitung
  - 5 Kriterien zur Einbindung von weiteren Subauftragsverarbeitern
- Kapitel 6: Auftragsverarbeitung außerhalb der EU / des EWR
  - 2 Kriterien zu Garantien für die Datenübermittlung in Drittstaaten
- Kapitel 7: Der Cloud-Anbieter als Verantwortlicher
  - 24 Kriterien zur Durchführung des Auftrags mit dem Cloud-Nutzer

AUDITOR-Kriterienkatalog – Entwicklung

Einarbeitung der Nachweise und Umsetzungshinweise:
Kriterienkatalog v. 0.2

Reflektion des TCDP-Katalogs:
Kriterienkatalog v. 0.1

1. Cloud-Anbieter Workshop:
Kriterienkatalog v. 0.8

Pilotierungen bei Cloud&Heat, Hornet Security & ecsec

Weiterentwicklung des Kriterienkatalogs für europ. Programmeinreichung

Katalog-Session:
Kriterienkatalog v. 0.4

2. Cloud-Anbieter Workshop:
Kriterienkatalog v. 0.9

Nationale Programmeinreichung bei DAkkS
Veröffentlichung des Kriterienkatalogs v. 0.99

Kriterienkatalog-Workshop
mit zahlreichen Teilnehmern:
Kriterienkatalog v. 0.7

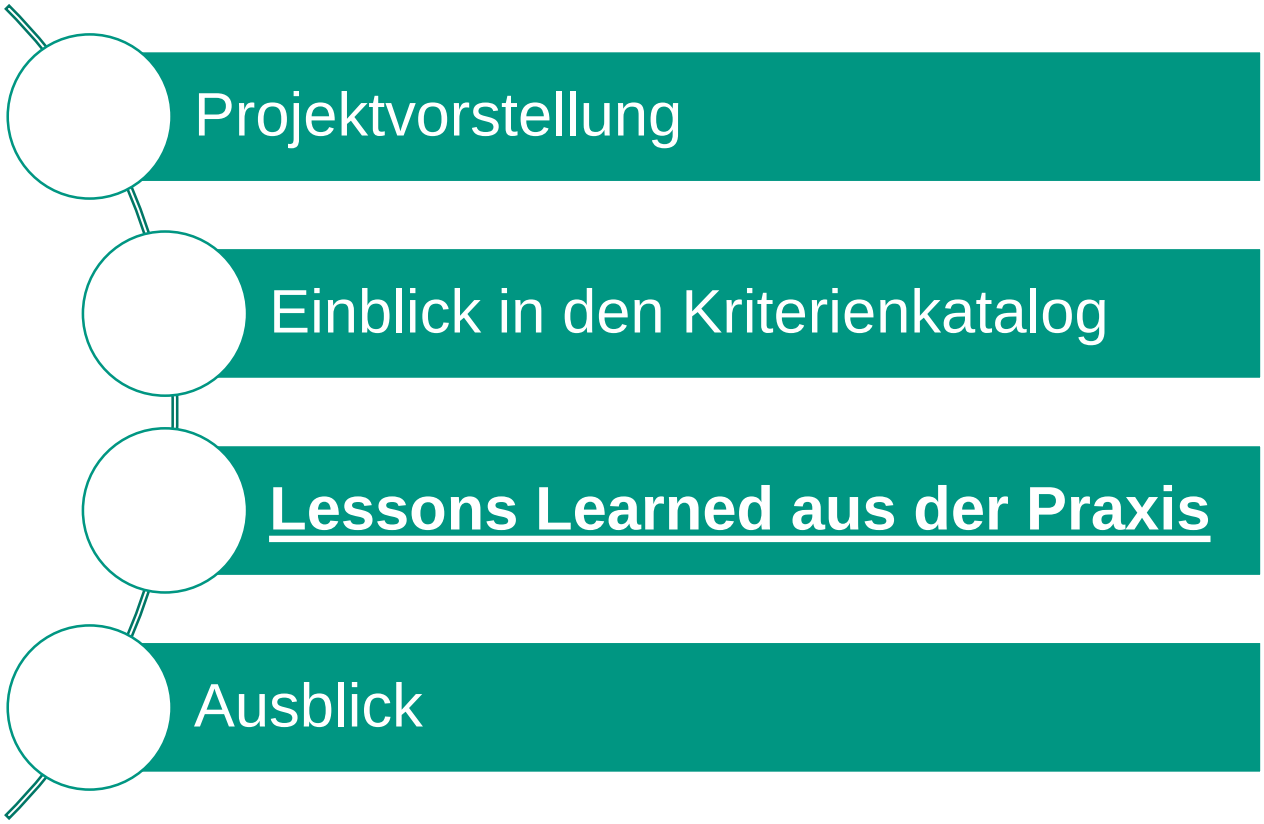
Veröffentlichung des Kriterienkatalogs v. 0.9
in dt. und engl. Sprache

AUDITOR-Kriterienkatalog – Europäisierung

Europäisches Datenschutzsiegel

- **Vorgabe in EDBP-Leitlinien 1/2018**: Den Datenschutzvorschriften der EU-Mitgliedstaaten muss Rechnung getragen werden
- **Kontaktierung der Aufsichtsbehörden** der EU-Mitgliedstaaten: Gibt es im nationalen Datenschutzrecht relevante Normen für Cloud-Anbieter?
- **Einholung von Gutachten** von nationalen Datenschutzexperten
- **Erstellung von Länderanhängen zum Kriterienkatalog** für 13 EU-Mitgliedstaaten

Agenda


Projektvorstellung
Einblick in den Kriterienkatalog
Lessons Learned aus der Praxis
Ausblick

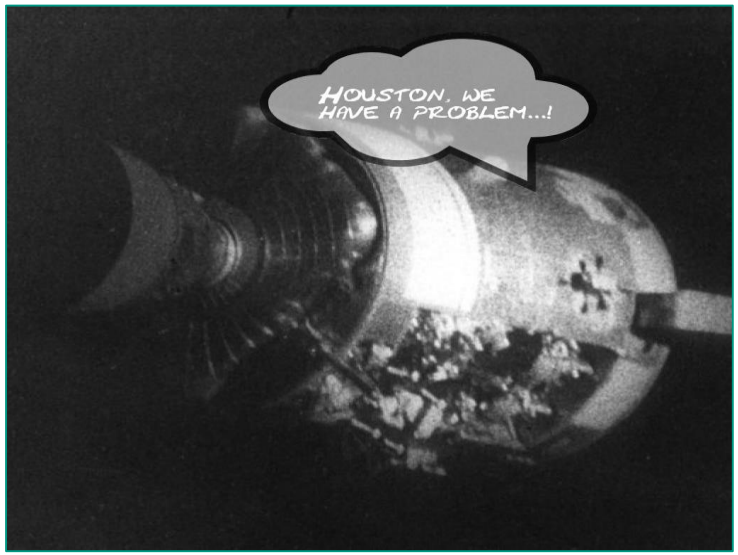
LESSONS LEARNED – ERFAHRUNGEN AUS DEN PILOT-AUDITS

Lessons Learned – Erfahrungen aus den Pilot-Audits

§ 9a Datenschutzaudit (BDSG alte Fassung):

- *„[…] Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen [können] ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen […].*

- *Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“*



Lessons Learned – Erfahrungen aus den Pilot-Audits

Bisher Zertifizierer mit proprietären Zertifikaten

- ULD
- EuroPriSe
- …
- …

- § 11 BDSG alt (Auftragsdatenverarbeitung)
- § 80 SGB X (Auftragsdatenverarbeitung)

Lessons Learned – Erfahrungen aus den Pilot-Audits

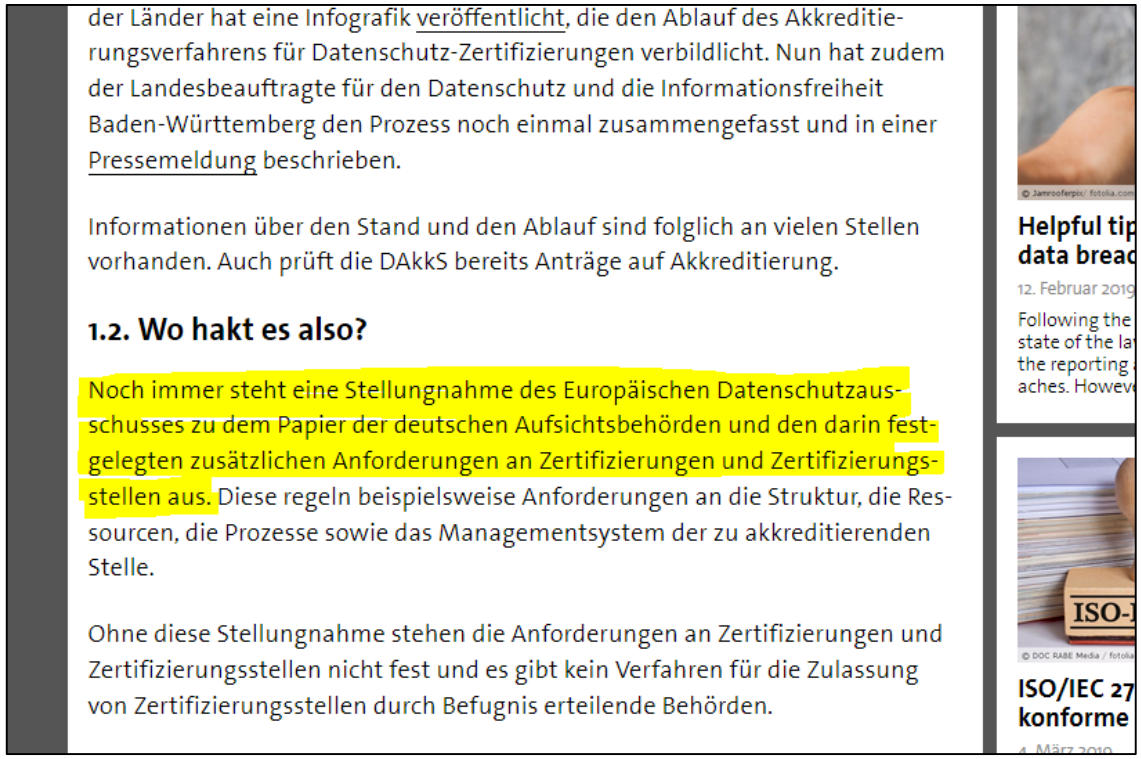
Art. 5 Abs. 2 DSGVO:

- *„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“*

Aber wie???

Lessons Learned – Erfahrungen aus den Pilot-Audits

Keine akkreditierten Zertifikate nach Art. 42/43 DSGVO – warum?



der Länder hat eine Infografik veröffentlicht, die den Ablauf des Akkreditierungsverfahrens für Datenschutz-Zertifizierungen verbildlicht. Nun hat zudem der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg den Prozess noch einmal zusammengefasst und in einer Pressemeldung beschrieben.

Informationen über den Stand und den Ablauf sind folglich an vielen Stellen vorhanden. Auch prüft die DAkkS bereits Anträge auf Akkreditierung.

1.2. Wo hakt es also?

Noch immer steht eine Stellungnahme des Europäischen Datenschutzausschusses zu dem Papier der deutschen Aufsichtsbehörden und den darin festgelegten zusätzlichen Anforderungen an Zertifizierungen und Zertifizierungsstellen aus. Diese regeln beispielsweise Anforderungen an die Struktur, die Ressourcen, die Prozesse sowie das Managementsystem der zu akkreditierenden Stelle.

Ohne diese Stellungnahme stehen die Anforderungen an Zertifizierungen und Zertifizierungsstellen nicht fest und es gibt kein Verfahren für die Zulassung von Zertifizierungsstellen durch Befugnis erteilende Behörden.

Helpful tip
data breac
12. Februar 2019
Following the
state of the la
the reporting
aches. Howev

ISO/IEC 27
konforme

Alisha Gühr, 23.05.2019 in datenschutz-notizen.de

Lessons Learned – Erfahrungen aus den Pilot-Audits

auditor

datenschutz cert

Ein Kommentar

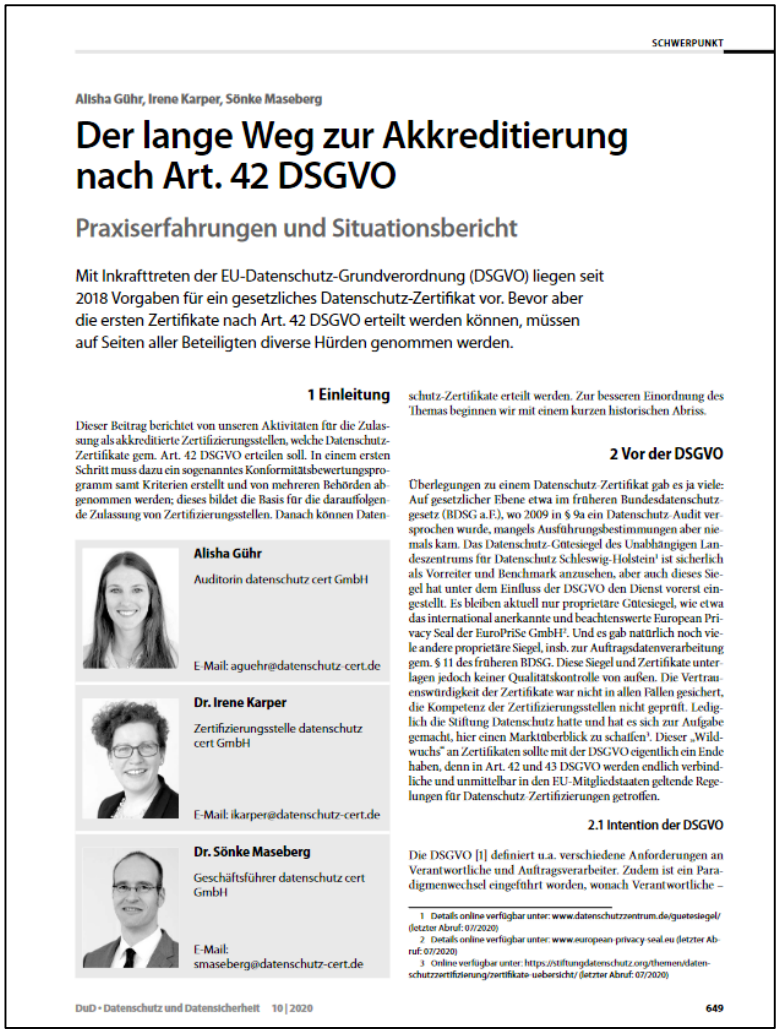
Anonymous

ANTWORTEN

23. MAI 2019 @ 10:39

Wäre es für uns Mittelständler nicht so ärgerlich wäre es ja noch lustig mit anzusehen wie die EU über ihre eigene Bürokratie stolpert. Für uns ist es Zeit- und Geldverschwendung, und gegenüber (potentiellen) Kunden die nicht nachfragen u.U. gar imageschädigend, immer wieder erklären zu müssen warum es keine Zertifikate mehr gibt. Mit großem Tamtam und angeblich ach so langer Vorlaufzeit wurde die DSGVO endgültig „scharfgeschaltet", so dass sich ja eigentlich niemand beschweren dürfe, aber fertig ist trotzdem nichts so richtig.

Lessons Learned – Erfahrungen aus den Pilot-Audits



SCHWERPUNKT

Alisha Gühr, Irene Karper, Sönke Maseberg

Der lange Weg zur Akkreditierung nach Art. 42 DSGVO

Praxiserfahrungen und Situationsbericht

Mit Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) liegen seit 2018 Vorgaben für ein gesetzliches Datenschutz-Zertifikat vor. Bevor aber die ersten Zertifikate nach Art. 42 DSGVO erteilt werden können, müssen auf Seiten aller Beteiligten diverse Hürden genommen werden.

1 Einleitung

Dieser Beitrag berichtet von unseren Aktivitäten für die Zulassung als akkreditierte Zertifizierungsstellen, welche Datenschutz-Zertifikate gem. Art. 42 DSGVO erteilen soll. In einem ersten Schritt muss dazu ein sogenanntes Konformitätsbewertungsprogramm samt Kriterien erstellt und von mehreren Behörden abgenommen werden; dieses bildet die Basis für die darauffolgende Zulassung von Zertifizierungsstellen. Danach können Datenschutz-Zertifikate erteilt werden. Zur besseren Einordnung des Themas beginnen wir mit einem kurzen historischen Abriss.

Alisha Gühr
Auditorin datenschutz cert GmbH
E-Mail: aguehr@datenschutz-cert.de

Dr. Irene Karper
Zertifizierungsstelle datenschutz cert GmbH
E-Mail: ikarper@datenschutz-cert.de

Dr. Sönke Maseberg
Geschäftsführer datenschutz cert GmbH
E-Mail: smaseberg@datenschutz-cert.de

2 Vor der DSGVO

Überlegungen zu einem Datenschutz-Zertifikat gab es ja viele: Auf gesetzlicher Ebene etwa im früheren Bundesdatenschutzgesetz (BDSG a.F.), wo 2009 in § 9a ein Datenschutz-Audit versprochen wurde, mangels Ausführungsbestimmungen aber niemals kam. Das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein[3] ist sicherlich als Vorreiter und Benchmark anzusehen, aber auch dieses Siegel hat unter dem Einfluss der DSGVO den Dienst vorerst eingestellt. Es bleiben aktuell nur proprietäre Gütesiegel, wie etwa das international anerkannte und beachtenswerte European Privacy Seal der EuroPriSe GmbH[2]. Und es gab natürlich noch viele andere proprietäre Siegel, insb. zur Auftragsdatenverarbeitung gem. § 11 des früheren BDSG. Diese Siegel und Zertifikate unterlagen jedoch keiner Qualitätskontrolle von außen. Die Vertrauenswürdigkeit der Zertifikate war nicht in allen Fällen gesichert, die Kompetenz der Zertifizierungsstellen nicht geprüft. Lediglich die Stiftung Datenschutz hatte und hat es sich zur Aufgabe gemacht, hier einen Marktüberblick zu schaffen[3]. Dieser „Wildwuchs" an Zertifikaten sollte mit der DSGVO eigentlich ein Ende haben, denn in Art. 42 und 43 DSGVO werden endlich verbindliche und unmittelbar in den EU-Mitgliedstaaten geltende Regelungen für Datenschutz-Zertifizierungen getroffen.

2.1 Intention der DSGVO

Die DSGVO [1] definiert u.a. verschiedene Anforderungen an Verantwortliche und Auftragsverarbeiter. Zudem ist ein Paradigmenwechsel eingeführt worden, wonach Verantwortliche –

1 Details online verfügbar unter: www.datenschutzzentrum.de/guetesiegel/ (letzter Abruf: 07/2020)
2 Details online verfügbar unter: www.european-privacy-seal.eu (letzter Abruf: 07/2020)
3 Online verfügbar unter: https://stiftungdatenschutz.org/themen/datenschutzzertifizierung/zertifikate-uebersicht/ (letzter Abruf: 07/2020)

https://www.datenschutz-notizen.de/wp-content/uploads/2020/09/Der_lange_Weg_zur_Akkreditierung_Art42DSGVO_DuD_10_2020.pdf

Lessons Learned – Erfahrungen aus den Pilot-Audits

Folgen

- Verantwortliche/Auftragsverarbeiter
  - AV-Prüfungen werden de facto kaum mehr durchgeführt, da die Aufwände z.Tl. kaum leistbar sind (Erfahrung aus vielen Audits)
  - Unsicherheit in Bezug auf Art. 5 DSGVO
- Betroffene
  - Auskunftsrechte tangiert
- Prüf- und Zertifizierungsstellen
  - können Datenschutz nicht abdecken
- Datenschutz blockiert sich derzeit selbst

Lessons Learned – Erfahrungen aus den Pilot-Audits

Nackte Zahlen…

- 3 Scopes (mit unterschiedlichen Verarbeitungsvorgängen)
- 4 Auditoren (2 juristisch/2 technisch)
- 16 Tage Site-Visits
- 21 Audit-Beteiligte
- 60 gesichtete Referenzdokumente
- 150 Tage Vor- und Nachbereitung
- 485 Seiten Berichte

Lessons Learned – Erfahrungen aus den Pilot-Audits

Vorbereitungen

- Nutzung etablierter Prozesse und Strukturen anderer Normen
  - Alte § 11 BDSG-Audits
  - ISO 27001 (Achtung anderer Blickwinkel: betrachtet Managementsystem)
- Erstellung von Berichtsvorlagen unter Berücksichtigung von
  - Kriterienkatalog
  - Konformitätsbewertungsprogramm
- Auditdokumentation
  - Agenda/Auditprogramm
  - Teilnehmerlisten
  - Auditbericht
  - Evaluation der Piloten (iterativer Prozess über drei Piloten)

Lessons Learned – Erfahrungen aus den Pilot-Audits

Prüf- und Zertifizierungsverfahren

- Aufgaben Prüfstelle
  - Planung Prüfverfahren
  - Sichtung Referenzdokumente im Vorfeld des Audits
  - Durchführung Prüfverfahren
  - Site-Visits
    - Interview
    - Einsichtnahme in Dokumente
    - Einsichtnahme in Systeme
    - Einsichtnahme in Betriebsdokumentationen etc.
  - Berichtserstellung mit Empfehlung an die Zertifizierungsstelle
- Aufgaben Zertifizierungsstelle
  - Prüfung und Abnahme Bericht
  - Ggf. Erteilung Zertifikat

Lessons Learned – Erfahrungen aus den Pilot-Audits

FIRMENVERTRAULICH

datenschutz cert

Inhaltsverzeichnis

FIRMENVERTRAULICH

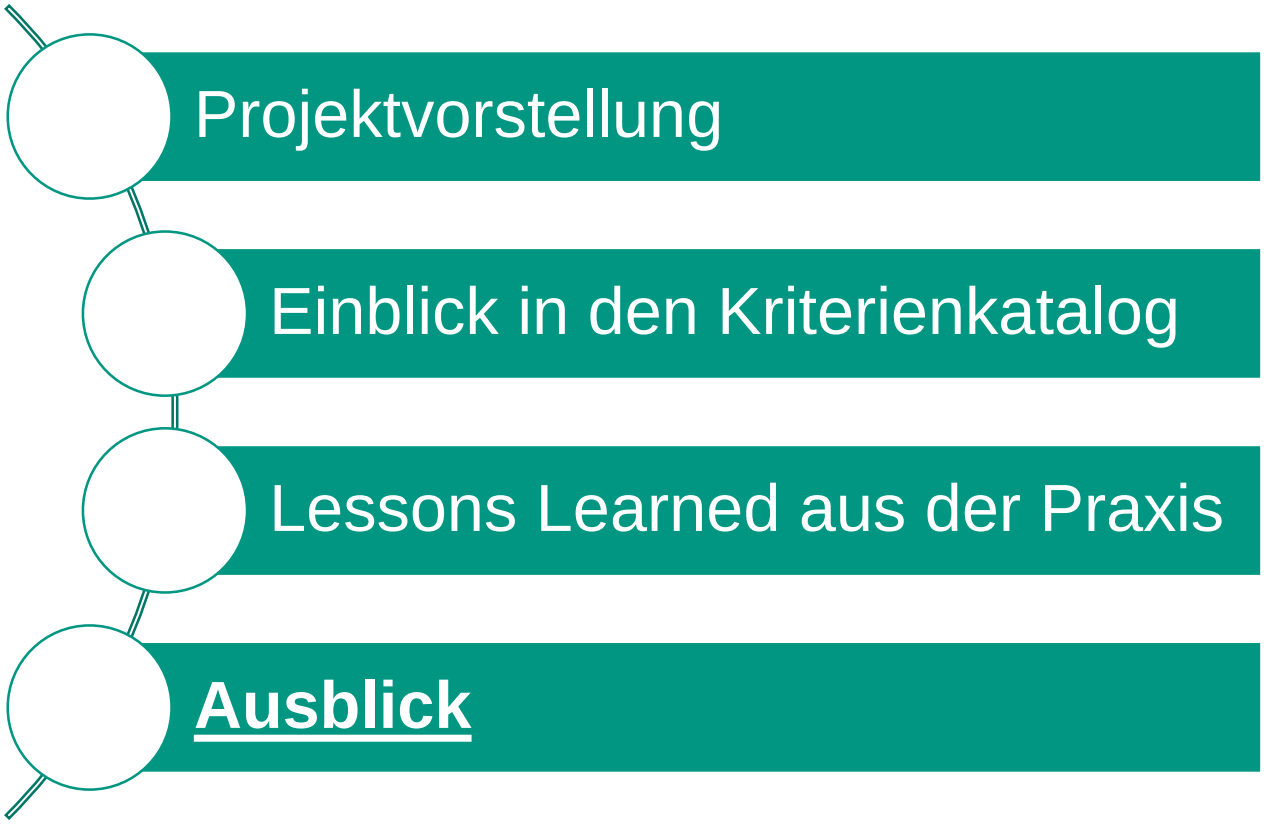
datenschutz cert

Lessons Learned – Erfahrungen aus den Pilot-Audits

Evaluation der Piloten

- Formal
- Verfahrenstechnisch
- Inhaltlich
  - Redundanzen
  - Innere Logik
  - Wording
- Juristisch
- Technisch
- Rückwirkung über Berichte und Auswertungen in das Projekt

Agenda


Projektvorstellung
Einblick in den Kriterienkatalog
Lessons Learned aus der Praxis
Ausblick

Verbreitung von AUDITOR: Zweistufiges Vorgehen

DAkkS Deutsche Akkreditierungsstelle

LDI NRW

edpb European Data Protection Board

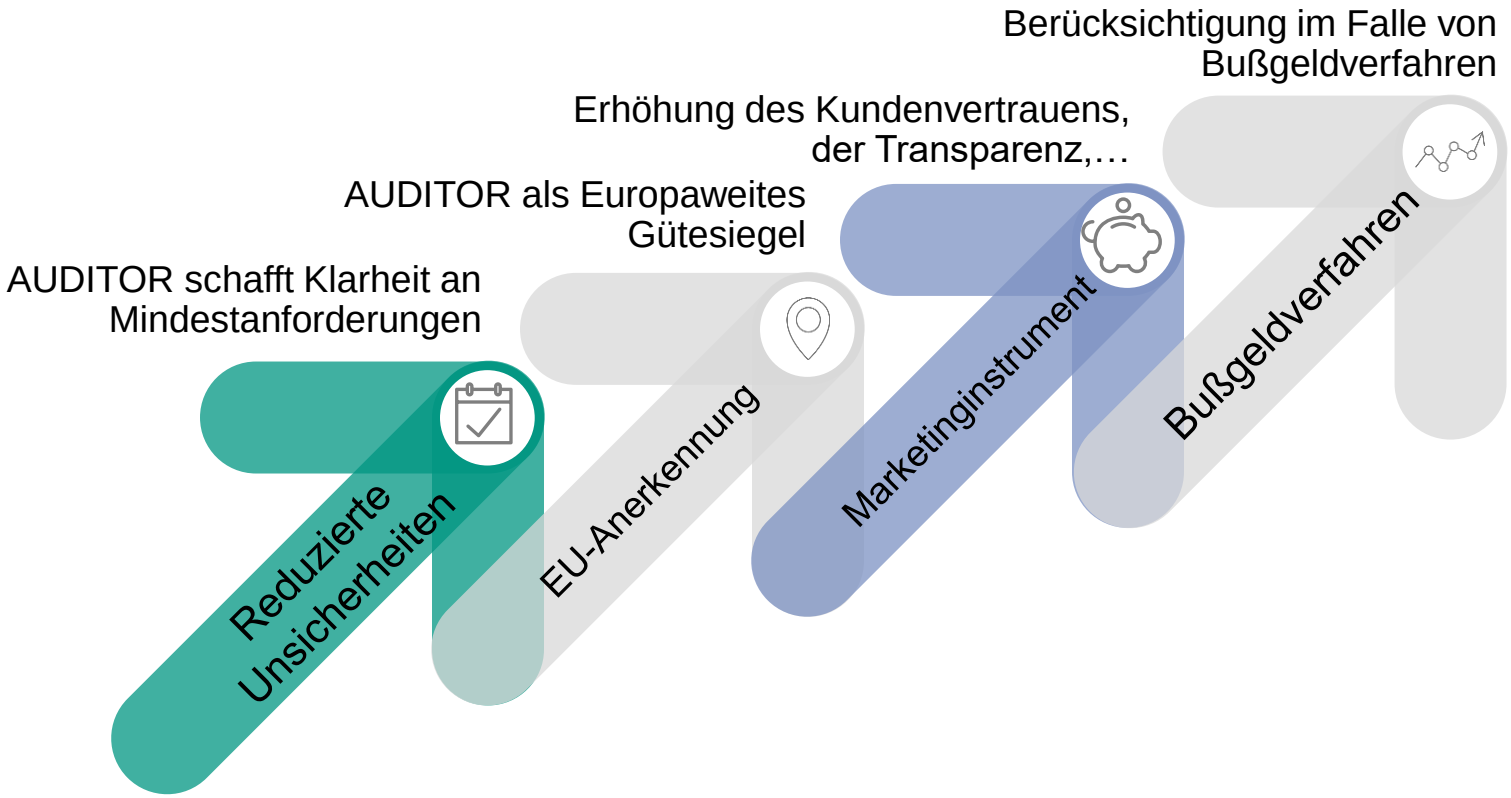
Nationale Anerkennung

- Entwicklung und Vorbereitung Genehmigung des Kriterienkatalogs durch Aufsichtsbehörden
- Vorbereitung der Akkreditierung des Programms bei DAkkS

Europaweite Anerkennung

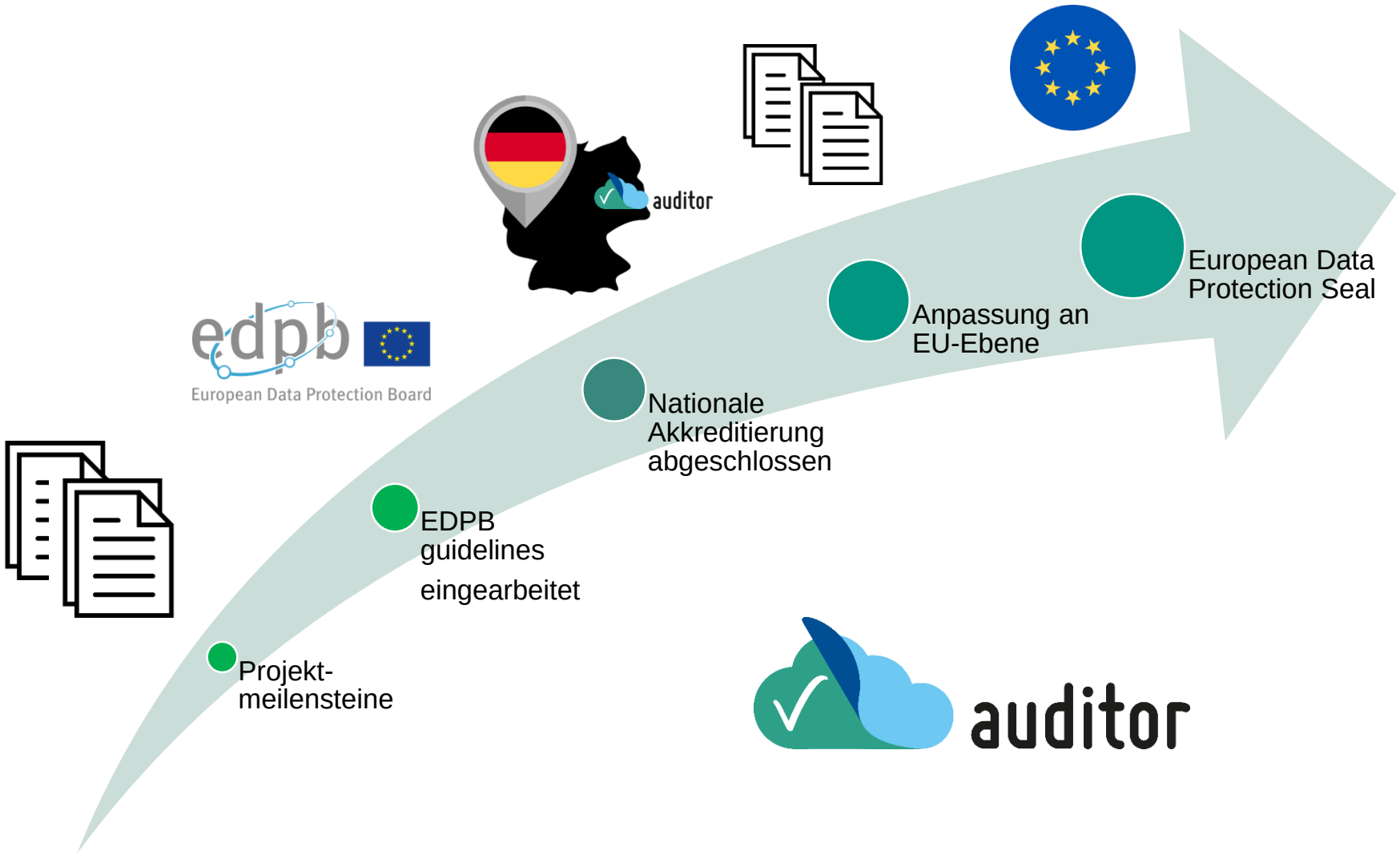
- Anpassung der Dokumente zur Entwicklung eines European Data Protection Seal
- Anerkennung durch den Ausschuss
- Akkreditierung der ZS und Genehmigung der Kriterien

Chancen durch die EU DSGVO
am Beispiel von AUDITOR



Durch AUDITOR können Cloud-Anbieter die **Vereinbarkeit** ihrer Datenverarbeitungsvorgänge **mit datenschutzrechtlichen Anforderungen der DSGVO** nachweisen

Zusammenfassung & Ausblick



Forschungsprojekt AUDITOR

European Cloud Service Data Protection Certification

Datenschutz am Mittag „Zertifizierung von Cloud-Diensten“
16.04.2021

Dr. Natalie Maier-Reinhardt, Universität Kassel
Kai Osterhage, datenschutz cert
Sebastian Lins, Karlsruher Institut für Technologie

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Status Quo: Ergebnisse von AUDITOR

Konformitäts-bewertungsprogramm 0.99b

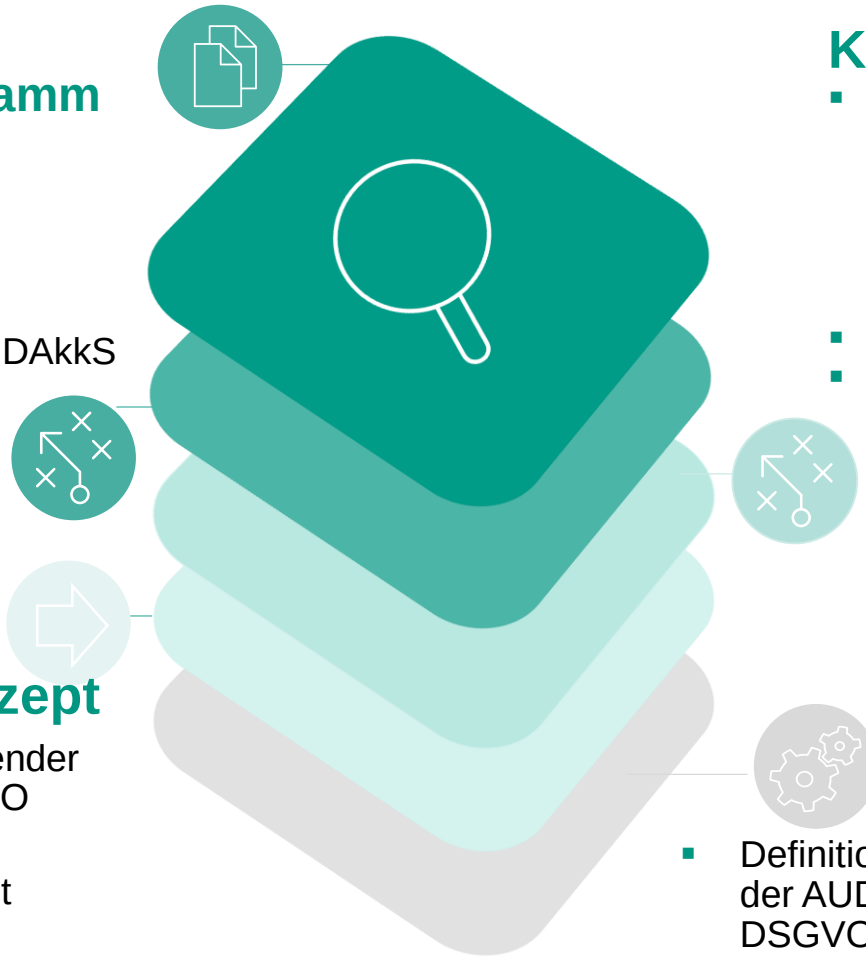
- Anforderungen an die Durchführung der Zertifizierung
- Ermittlungsmethoden
- Enge Abstimmung mit DAkkS

DIN-SPEC

- Erarbeitung des Kriterienkatalogs als DIN-SPEC 27557

Modularitätskonzept

- Anerkennung bestehender Zertifizierung, insb. ISO 270XX
- Schutzklassenkonzept



Kriterienkatalog 0.99b

- beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers
- Rolle des Auftragsverarbeiters
- Rolle des Verantwortlichen

Zertifizierungs-gegenstand

- Definition des Bewertungsgegenstandes der AUDITOR-Zertifizierung gem. DSGVO
- **Verarbeitungsvorgänge**, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten oder Diensten erbracht werden

Breite Öffentlichkeitswirkung

Verwaltung & Lizensierung

Verwaltung von AUDITOR

Das **Kompetenznetzwerk Trusted Cloud e.V.** verwaltet AUDITOR **als Programmeigner**

Folgende Tätigkeiten werden durchgeführt:

- Durchführung von Änderungen an Zertifizierungskriterien
- Leitung der Standardisierung
- Änderungen am Programm
- Marktbeobachtungen
- Koordination Europäisierung
- …

Einrichtung eines Beirats mit Vertretern von

- Karlsruher Institut für Technologie,
- Universität Kassel,
- BMWi
- …

Lizensierung von AUDITOR

Jede Zertifizierungsstelle kann nach AUDITOR zertifizieren

Zertifizierungsstellen müssen sich nach der **ISO/IEC 17065** i.V.m. den **ergänzenden Anforderungen** zur Akkreditierung nach Art. 43 Abs. 3 DSGVO **und dem AUDITOR-Programm akkreditieren** lassen

Zur Nutzung des AUDITOR-Gütesiegels wird ein Lizenzvertrag mit Trusted Cloud geschlossen

Zertifizierungsgegenstand

Akkreditierungspflicht

Akkreditierungspflicht gemäß Art. 43 Abs. 1 DSGVO:
Die Mitgliedstaaten stellen sicher, dass Zertifizierungsstellen akkreditiert werden

Was bedeutet ‚Akkreditierung'?

DAkkS Deutsche Akkreditierungsstelle

Zertifizierungsstellen weisen gegenüber einer **unabhängigen Akkreditierungsstelle** nach, dass sie ihre Tätigkeiten **fachlich kompetent**, unter Beachtung gesetzlicher sowie normativer Anforderungen und auf **international vergleichbarem Niveau** erbringen

Änderung des Akkreditierungs-stellengesetztes

Die DAkkS kann seit Dez. 2018 mittels **Untersagungs-verfügungen Zertifizierungen ohne Akkreditierung** Einhalt gebieten

www.dakks.de/content/novelle-des-akkreditierungsstellengesetz-kraft-getreten

Konformitätsbewertung

- 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 Deutsche Akkreditierungsstelle GmbH (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 Datenschutzkonferenz (DSK) zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065
- Maßgeblich für die Akkreditierung ist ein Konformitätsbewertungsprogramm (KBP), das für jedes Zertifizierungsverfahren erstellt werden muss

AUDITOR-Konformitätsbewertungsprogramm

Das AUDITOR-KBP beschreibt gemäß Art. 43 Abs. 2 DSGVO:

- die von der Zertifizierungsstelle zu erfüllenden Grundsätze
  - Unparteilichkeit, Kompetenz, Vertraulichkeit, Offenheit…
- Anforderungen an die Zertifizierungsstelle
  - Akkreditierung, notwendige Struktur und Ressourcen, Managementsystemanforderungen…
- Anforderungen an den Zertifizierungsprozess
  - Auswahl (Zertifizierungsvereinbarung…), Ermittlung (Methoden und Objekte…), Bewertung (Nichtkonformität…), Entscheidung, Bestätigung (Erteilung Zertifikat), Überwachung
- Festlegung der Prüfung der einzelnen Kriterien (Ermittlungsmethoden)
  - Audit, Dokumentenprüfung, Entwicklungs- und Designprüfung…

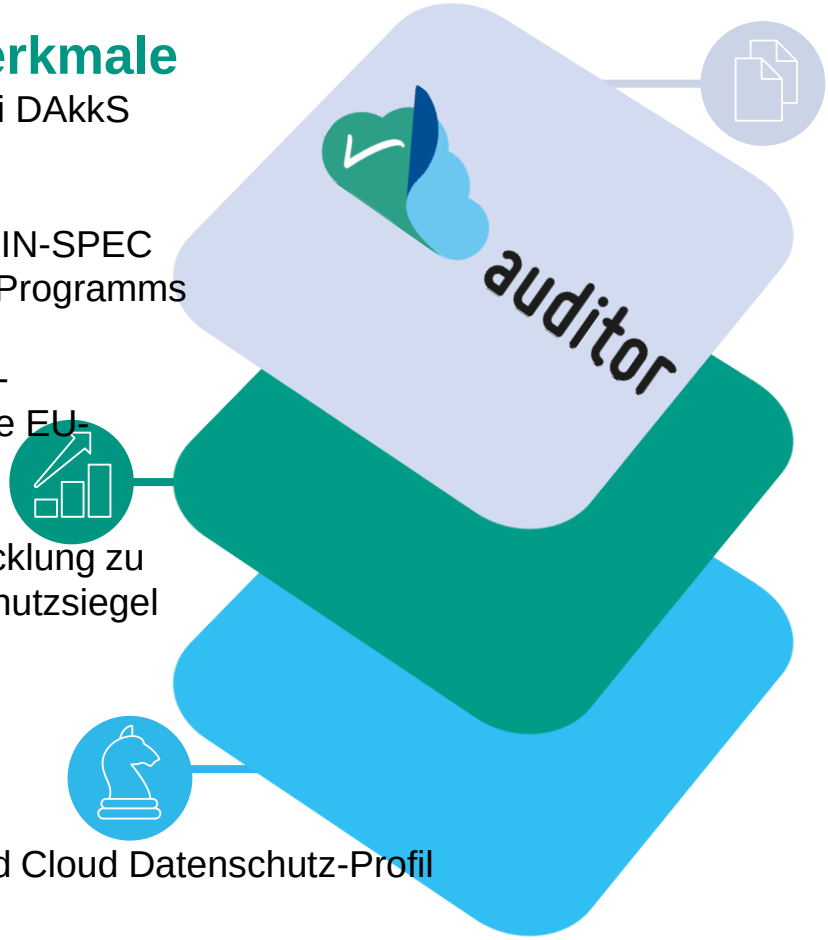
Ablauf Akkreditierungsprozess

Antragsphase	Programmeigner (scheme owner) zur Anmeldung festlegen
Einbindung der Aufsicht	Informierung der Aufsichtsbehörden
Prüfungsphase	Bewertung des Programms erfolgt anhand der DAkkS-Checkliste, der Unterlagen und des Validierungsberichtes
Beseitigung von Abweichungen	die festgestellten Abweichungen beheben oder zu den Abweichungen Stellung nehmen
Bewertung und Entscheidung im Programmausschuss	der Programmausschuss entscheidet über die Akkreditierungsfähigkeit des Programms
Bescheinigung/Ablehnung der Feststellung der Akkreditierungsfähigkeit	Mitteilung Entscheidung

Marktpotenzial

Alleinstellungsmerkmale

- Einziges Pilotprojekt bei DAkkS
- Unterstützung durch Aufsichtsbehörden
- Parallele Entwicklung DIN-SPEC
- Frühe Einreichung des Programms im Februar 2020
- Befürwortung durch EU-Kommission und weitere EU-Länder
- Zukünftige Weiterentwicklung zu europäischem Datenschutzsiegel
- …



Abgrenzung zu Code of Conducts (CoC)

- Zertifizierungsprozess statt nur Bekennung zur Einhaltung des CoC
- Externe, unabhängige Prüfung im Rahmen der initialen Zertifizierung und
- Überwachung der Zertifizierungseinhaltung
- Stärkere Berücksichtigung bei Beurteilung von Datenschutzvorfällen und Bußgeldern
- …

Vorteile

- Aufbau auf dem Trusted Cloud Datenschutz-Profil
- Interdisziplinäres Team
- Hohe Marktakzeptanz durch Einbindung aller Stakeholder am Markt
- Offene Bereitstellung der Ergebnisdokumente
- Durchführung von Pilotzertifizierungen zur Validierung
- …

Abgrenzung zur ISO/IEC 27701

- **ISO/IEC 27701 ist keine DSGVO-konforme Zertifizierung!**
- Mit der Norm ISO/IEC 27701 „Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden“, die vor kurzem veröffentlicht wurde, lässt sich ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 wunderbar um Datenschutz-Aspekte ergänzen

→ Datenschutzmanagementsystem

- ISO/IEC 27701 ist keine Zertifizierungsnorm. Zertifiziert wird stets ein ISMS gem. ISO/IEC 27001.

- KEINE zugelassene Norm für DSGVO-Compliance
  - DSGVO hat die Akkreditierungsnorm ISO/IEC 17065 für Produkte und Dienstleistungen vorgegeben (Zertifizierungsgegenstand sind Verarbeitungsvorgänge)
  - ISO/IEC 27001 zählt zu den sogenannten Managementsystemnormen (ISO/IEC 17021)

- Analog gilt gleiches für BS 10012:217 (British Standards Institute, BSI)

Expertenbeirat

Technische Universität München

Prof. Dr. Helmut Krcmar, Lehrstuhl für Wirtschaftsinformatik, Technische Universität München

UNIVERSITÄT DES SAARLANDES

Prof. Dr. Georg Borges, Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie, Universität des Saarlandes

STIFTUNG DATENSCHUTZ

Frederick Richter, LL.M., Stiftung Datenschutz

DVD Deutsche Vereinigung für Datenschutz e. V.

Dr. Thilo Weichert, Deutsche Vereinigung für Datenschutz e. V.

bitkom

Susanne Dehmel, Bitkom e.V.

Steuerungsgremium / Lenkungsausschuss

u.a.

DAkkS Deutsche Akkreditierungsstelle

Bundesministerium für Wirtschaft und Energie

Bundesministerium des Innern, für Bau und Heimat

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit