

IT-Sicherheitsrechtstag 2018

TeleTrust – Bundesverband IT-Sicherheit e.V.

Berlin, 25.10.2018

Akkreditierungen von Zertifizierungsstellen nach DS-GVO

Dr. iur. Raoul Kirmes, M.Sc.

Ingenieur für Informationssicherheitstechnik

Deutsche Akkreditierungsstelle GmbH (DAkkS)

Übersicht

1. DAkkS = Nationale Akkreditierungsstelle
2. „Akkreditierung“ nach Art. 43 Abs. 1 DS-GVO
3. Ablauf des Akkreditierungsverfahrens § 39 BDSG
4. „Anforderungen“ n. Art. 43 Abs. 3 DS-GVO
5. „Kriterien“ n. Art. 42 Abs. 5 DS-GVO als Teil der Konformitätsbewertungsprogramme
6. Anforderungen an ein „Zertifizierungsprogramm“



1. DAkkS = Nationale Akkreditierungsstelle



Nationale Akkreditierungsstelle (DAkkS)



- **Einzige nationale** Akkreditierungsstelle mit **europäischer und internationaler Anerkennung** für Deutschland
- **Sicherstellung hoher Qualität aller Konformitätsbewertungen im Bereich 3rd-Party**
- **Zeit- und qualitätsgerechte** Bereitstellung von Akkreditierungen (**Kompetenzfeststellung**)
- **Laufende Überwachung** der **fachlichen Kompetenz** und **Unabhängigkeit** der Stellen
- **Abbau von Handelshemmnissen** aus Konformitätsbewertungen (Zertifikaten, etc.) in **Europa** und im Handel mit **Drittstaaten**

DAkkS: Eckdaten

3

Standorte
(B, BS, FfM)

rd. **180** Mitarbeiter
rd. **1.030**
externe Begutachter/
Fachexperten

6 Fachabteilungen

47 Fachbereiche

34

Sektorkomitees

rd. **4.100**
**Akkreditierungs-
urkunden**

seit **2010** tätig
(gesetzliche
Grundlage
AkkStelleG)

Beispiele für Konformitätsbewertungsstellen





2. Akkreditierung nach Art 43 DS-GVO

Art. 43 Abs. 1 EU-DSGVO (Akkreditierung)

Verweis auf NLF-System der EU

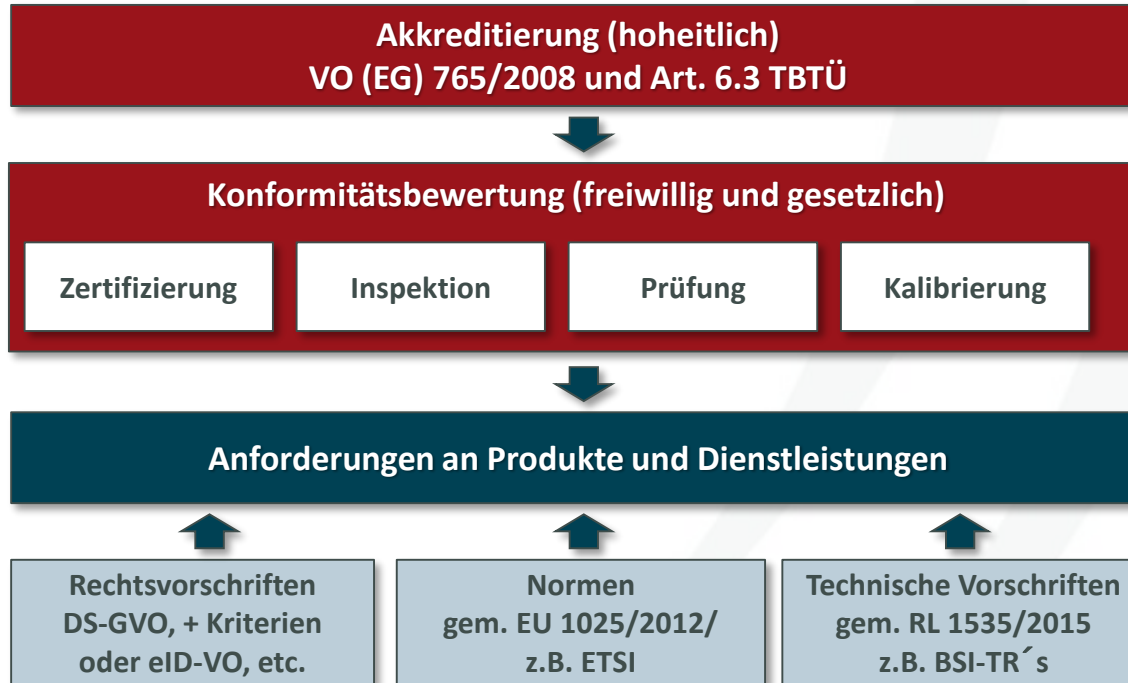
Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde (...) erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde (...) die Zertifizierung.

Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von **einer oder beiden** der folgenden Stellen akkreditiert werden:

- der **gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde**;
- der **nationalen Akkreditierungsstelle**, die gemäß der Verordnung (EG) **Nr. 765/2008** (..) im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der (...) zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.

Horizontale Qualitätsinfrastruktur

Akkreditierung im 3 Ebenen System der Konformitätsbewertung



Horizontaler Rechtsrahmen des New Legislative Framework (NLF)



Europäische Ebene

Verordnung (EG) Nr. 765/2008

Verordnung (EG) Nr. 764/2008

Beschluss (EG) Nr. 768/2008

Verordnung (EU) Nr. 1025/2012

**Informationsrichtlinie
1535/2015 EU**

**Vergaberichtlinie
Art. 44 2014/24/EU**

Nationale Ebene



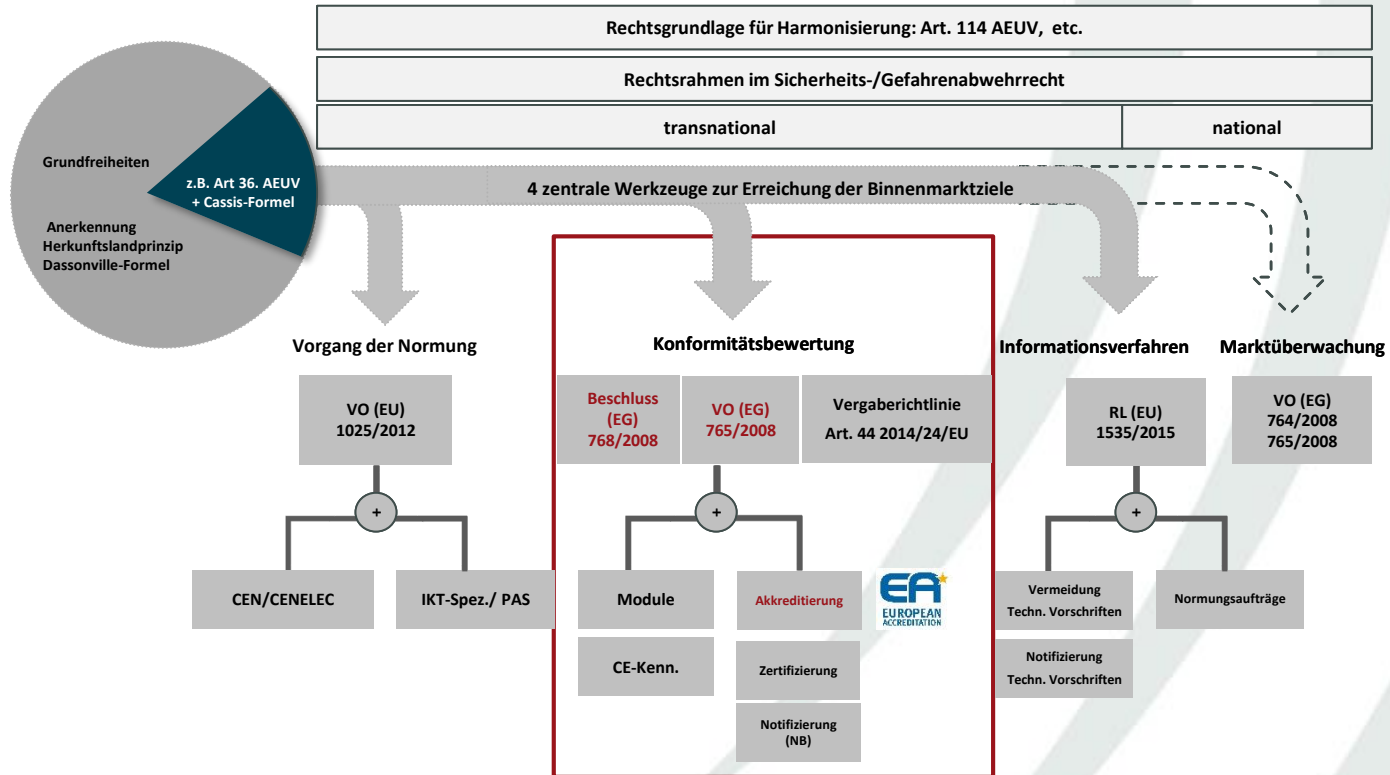
**Akkreditierungsstellengesetz
(AkkStelleG)**

**Beleihungsverordnung
(AkkStelleGBV)**

Gebührenverordnung

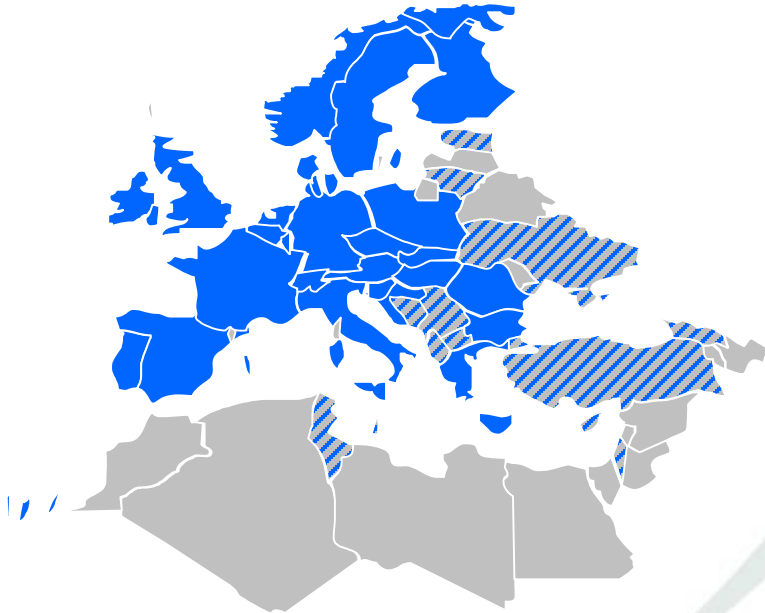
**Akkreditierungssymbolverordnung
(SymbolVO)**

Konformitätsbewertung im NLF



Europaweite Anerkennungspflicht

Art. 11 II VO (EG)765/2008; Art. 5 (EG) 764/2008

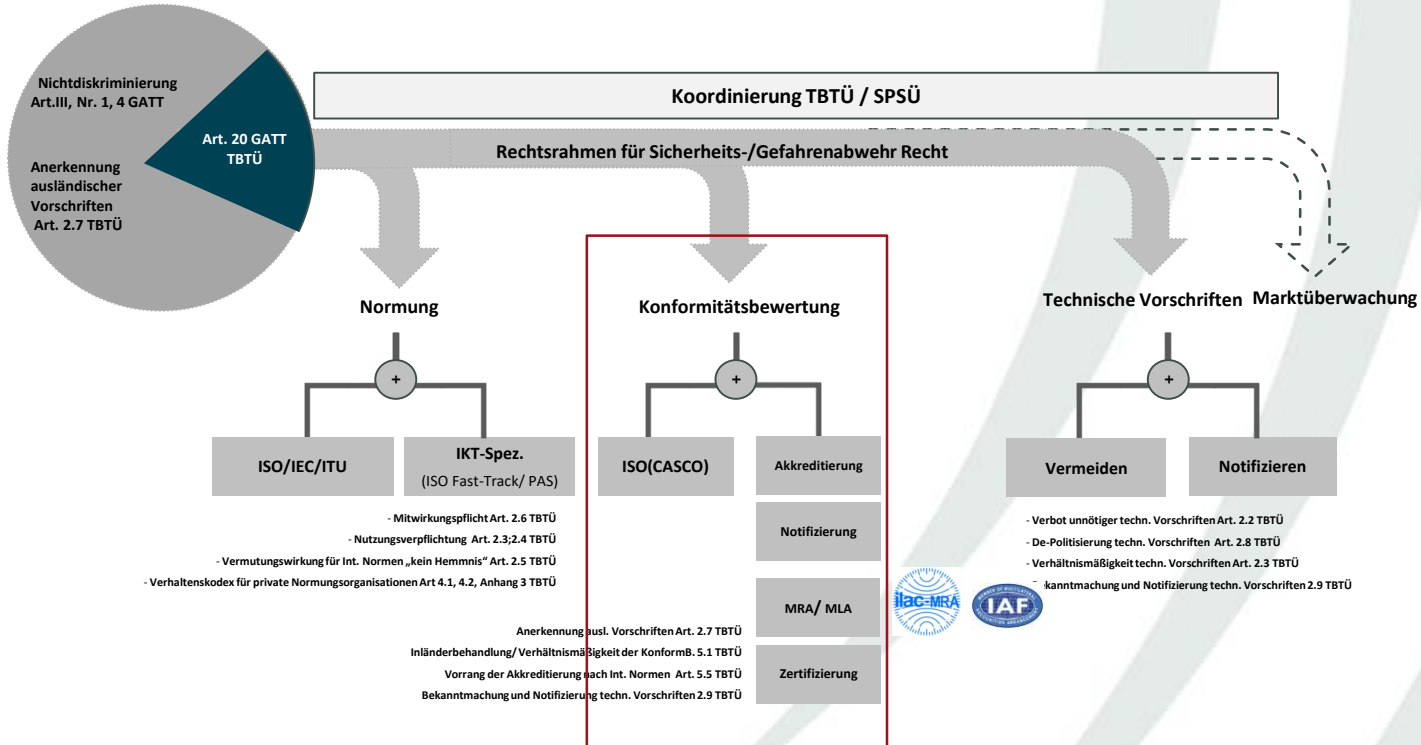


Accreditation of Scope/Activity:		Standard
Laboratories	Testing and Medical examinations	ISO 17025
	Calibration	ISO 15189
Certification Bodies	Product certification	ISO 17025
	Certification of persons	ISO 17065
	Management systems certification	ISO 17024
Inspection	Inspection	ISO 17021
Validation and verification		ISO 17020
Proficiency Testing Providers (PTP)		EN 14065
		ISO 17043

Full MLA

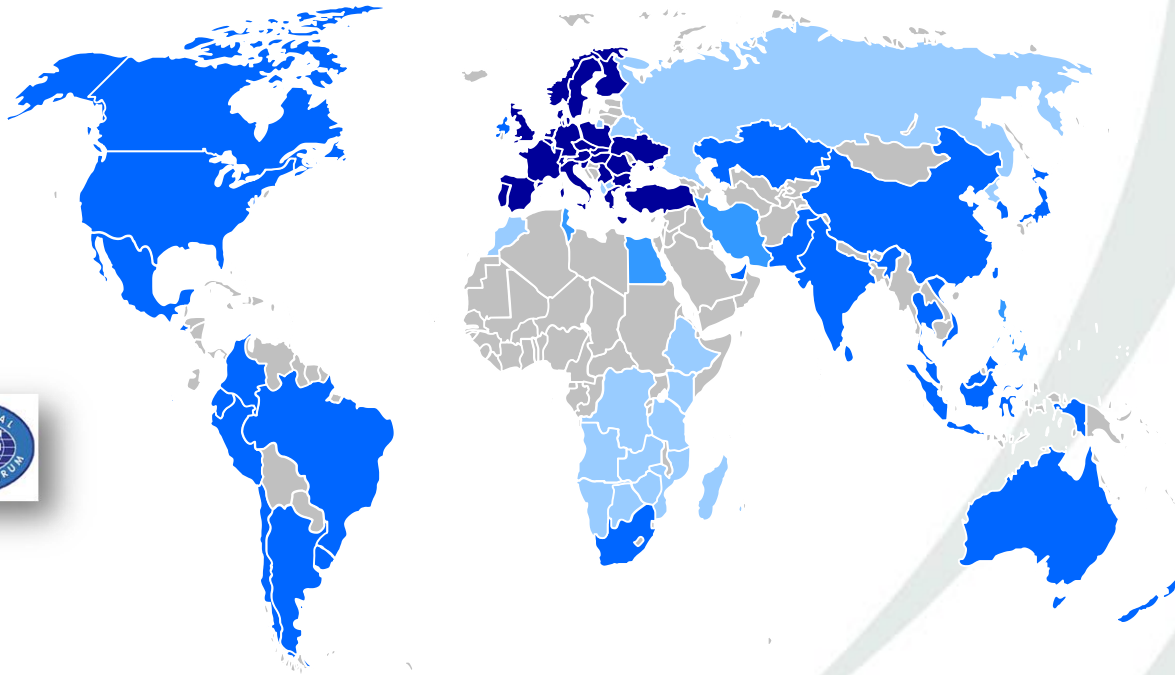
BLA-Member

Konformitätsbewertung im WTO-Recht



Weltweite Anerkennung durch IAF-Abkommen

Art. 6 Agreement on Technical Barriers to Trade (TBT)

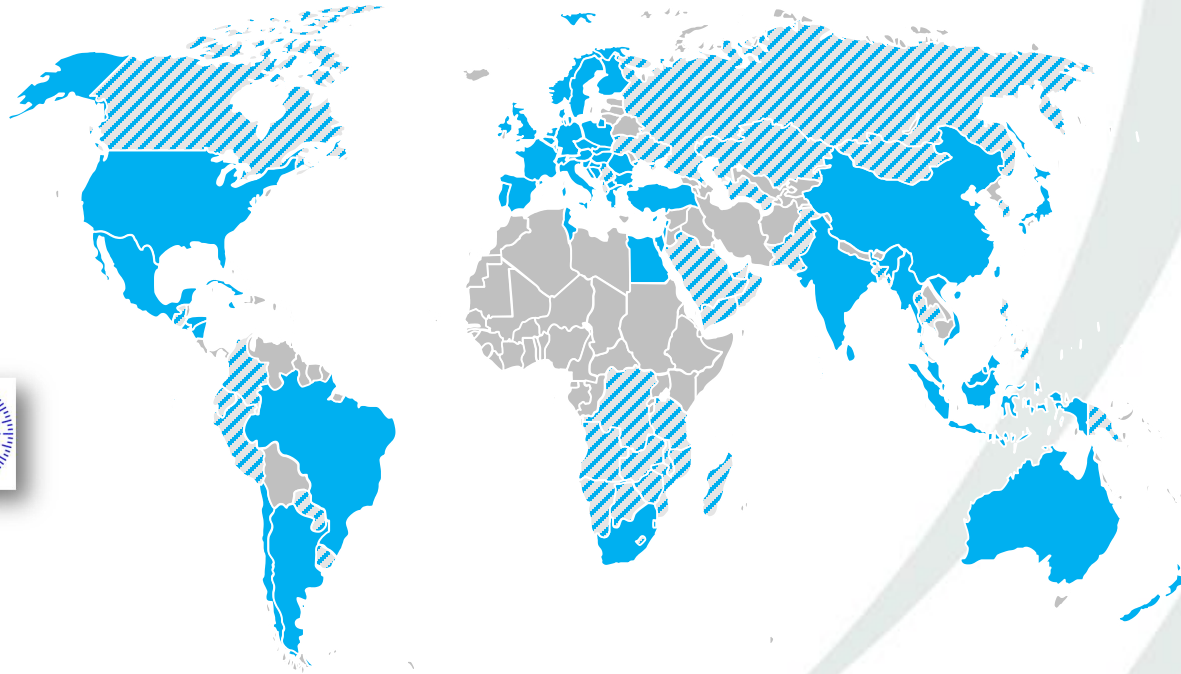


Management systems:	ISO 17021
Product certifications:	ISO 17065
Certification of persons:	ISO 17024
Greenhouse Gas	
Validation and Verification	ISO 14065

Member without MLA		
17021		
17021	17065	
17021	17065	17024

Weltweite Anerkennung durch ILAC-Abkommen

Art. 6 Agreement on Technical Barriers to Trade (TBT)



Medical Testing:	ISO 15189
Inspection:	ISO 17020
Testing:	ISO 17025
Calibration:	ISO 17025

Full MRA
Partial MRA



3. Ablauf des Akkreditierung/Befugnis

39 BDSG (Akkreditierung)

Umsetzung in Deutschland: bewährter Rückgriff auf AkkStelleG

Die **Erteilung der Befugnis**, als Zertifizierungsstelle gemäß **Artikel 43 Absatz 1 Satz 1 der Verordnung (EU) 2016/679** tätig zu werden, erfolgt durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige **Aufsichtsbehörde des Bundes oder der Länder** auf der **Grundlage einer Akkreditierung** durch die **Deutsche Akkreditierungsstelle**.
§ 2 Absatz 3 Satz 2, § 4 Absatz 3 und § 10 Absatz 1 Satz 1 Nummer 3 des Akkreditierungsstellengesetzes finden mit der Maßgabe Anwendung, dass der **Datenschutz als ein dem Anwendungsbereich des § 1 Absatz 2 Satz 2 unterfallender Bereich** gilt.

Duales System des AkkStelleG

Bereiche ohne Befugniserteilung

Horizontaler Grundsatz

§ 1 Abs. 1 AkStelleG

„Die Akkreditierung wird als hoheitliche Aufgabe des Bundes durch die Akkreditierungsstelle durchgeführt.“

Stets in allen Bereichen zu verwenden wenn kein EU-Rechtsakt oder (EU-rechtskonformes) nationales Gesetz Abweichung zulässt.

Bereiche mit Befugniserteilung

Sektorale Ausnahmen

§ 1 Abs. 2 AkStelleG

- Medizinprodukte
- Gendiagnostika
- Sicherheitstechnik
- Ernährung
- Landwirtschaft Verbraucherschutz
- Lebensmittelsicherheit

**Neu durch DSAnpUG-EU in § 39 BDSG:
Datenschutz ist Bereich nach
§ 1 Abs. 2 AkkStelleG**

Bewährtes 2-Stufen-System

ISO/IEC 17011
Genehmigte Anforderungen
ISO/IEC 17065
Genehmigte Kriterien

1. Stufe:
**Akkreditierung
durch DAkkS**

Kompetenzfeststellung
(„**fachliches Können**“)

2. Stufe:
**Befugniserteilung
durch
Datenschutz-
behörde**

Erlaubnis
(„**rechtliches Dürfen**“)

Vgl. ISO/IEC 17000

Tätigkeit der KBS

=

Konformitätsaussagen
zu den Anforderungen
der EU-DSGVO



4. „Anforderungen“ nach Art 43 DS-GVO

Art. 43 Abs. 3 EUDSGVO (IAF/EA **Level 1**)

„Die **Akkreditierung** von **Zertifizierungsstellen** nach den Absätzen 1 und 2 erfolgt anhand der **Anforderungen**, die von der gemäß Artikel 55 oder 56 **zuständigen Aufsichtsbehörde** **[National!] oder** — gemäß Artikel 63 — von dem **Ausschuss genehmigt** wurden.

Im Fall einer Akkreditierung nach Absatz 1 Buchstabe b des vorliegenden Artikels **ergänzen** **diese Anforderungen** diejenigen, die in der **Verordnung (EG) Nr. 765/2008** und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.“

Anforderungen nach Art. 43 Abs. 3 EUDSGVO (IAF/EA **Level 1**)

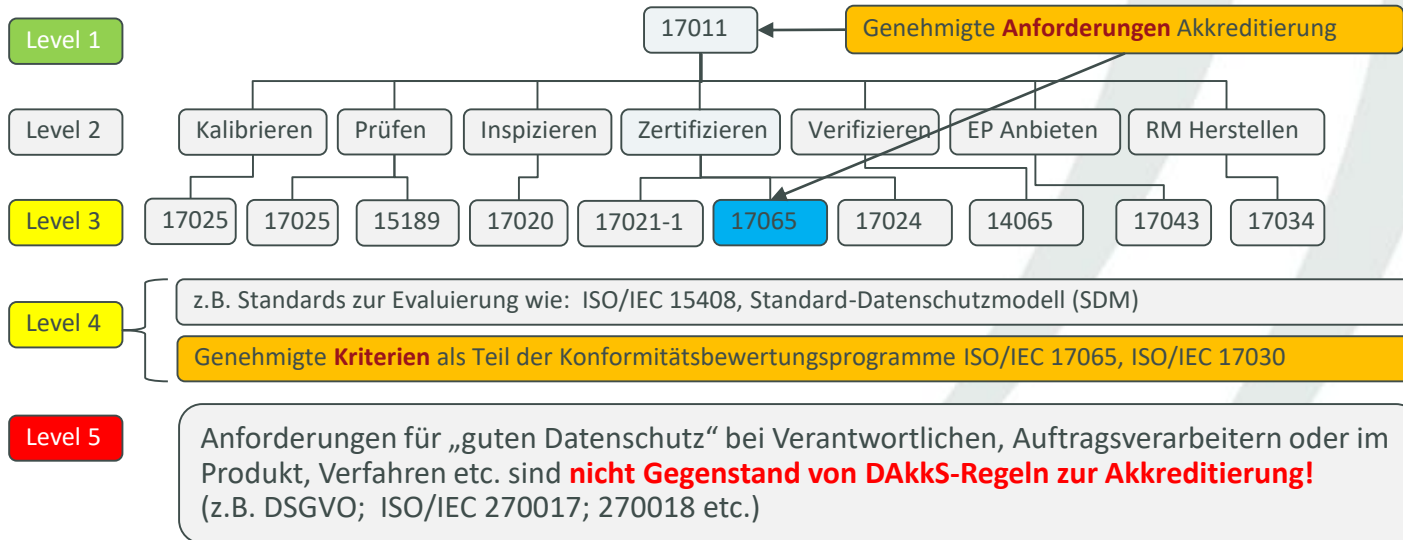
„**Ergänzen**“ diejenigen, die in der Verordnung (EG) Nr. 765/2008“

also insbesondere: ISO/IEC 17011

- + ISO/IEC 17000**
- + IAF – Dokumente**
- + EA – Dokumente**
- + DAkkS-Regeln**

Art. 43 Abs. 3 EUDSGVO (IAF/EA **Level 1**)

„Anforderungen“ im normativen Akkreditierungssystem



Aktueller Stand zu den „Anforderungen“

- Sind durch die DSK genehmigt und werden als Entwurf veröffentlicht
- Finale Version wird nach Genehmigung oder Fristablauf durch den Europäischen Ausschuss veröffentlicht
- Nach Veröffentlichung der Draft Version wird die Programmprüfung bei der DAkkS und im Rahmen dieser die Genehmigung der „Kriterien“ bei den Datenschutz-Aufsichtsbehörden veröffentlicht



5. Art 42 Abs. 5 DS-GVO „Kriterien“ als Teil der Konformitätsbewertungsprogramme (IAF **Level 4 - 5)**

Art. 42 Abs. 5 EU-DSGVO (IAF/EA Level 4-5)

„Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 **[Nationale Datenschutzbehörde!]** oder — gemäß Artikel 63 — durch den Ausschuss **genehmigten Kriterien** erteilt.

Werden die Kriterien vom Ausschuss genehmigt, **kann** dies zu einer gemeinsamen Zertifizierung, dem **Europäischen Datenschutzsiegel**, führen.“

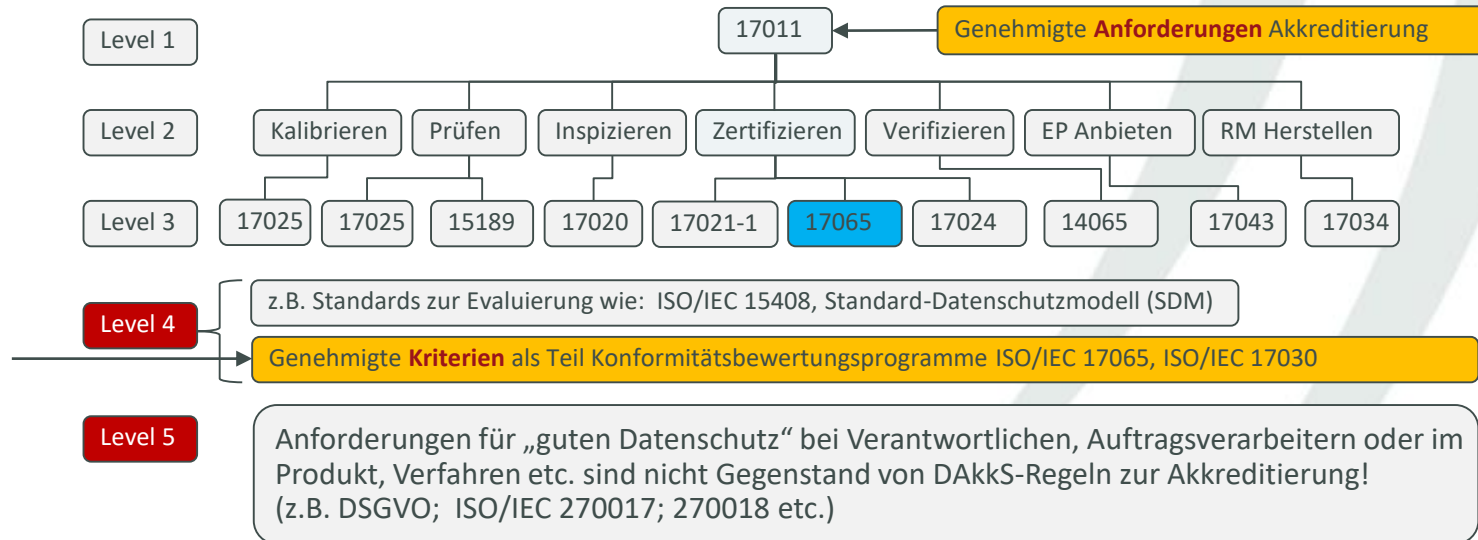
Kein WARTEN auf den Ausschuss.

Regeln des Ausschusses ersetzen nicht die nationalen Regeln.

Sie führen nur zu einem besonderen Gütesiegel!

Art. 42 Abs. 5 EU-DSGVO (IAF **Level 4-5**)

„**Kriterien**“ im normativen Akkreditierungssystem



Art. 42 Abs. 5 EU-DSGVO (IAF **Level 4-5**)

Verfahrensablauf zu den „genehmigten Kriterien“

1. Antrag durch Konformitätsbewertungsstelle **bei Programmprüfungsstelle der DAkkS auf Feststellung der Akkreditierungsfähigkeit des Konformitätsbewertungsprogramms.**
2. Die DAkkS stellt zunächst fest, ob das Konformitätsbewertungsprogramm die Anforderungen der ISO/IEC 17000 Anhang A, ISO/IEC 17007, ISO/IEC 17065 und 17067, 17030 usw. (vgl. **DAkkS-Regel 71 SD 0 016**) erfüllt, um in der Akkreditierung eingesetzt zu werden (Feststellung der Akkreditierungsfähigkeit des Programms). **Dabei werden die MA der Datenschutzaufsicht als Fachbegutachter der BeB gemäß AkkStelleG eingesetzt.** Insbesondere zur Beurteilung der Eignung von Kriterien auf Level 5.
3. Bei positivem DAkkS-Votum und anschließender **Genehmigung** der Datenschutzaufsicht kann dieses Programm Grundlage einer Akkreditierung werden. Kein positiver Bescheid DAkkS ohne vorherige Genehmigung der Aufsichtsbehörde.



6. „Anforderungen“ an Zertifizierungsprogramme

Ein Zertifizierungsprogramm setzt sich zusammen aus:

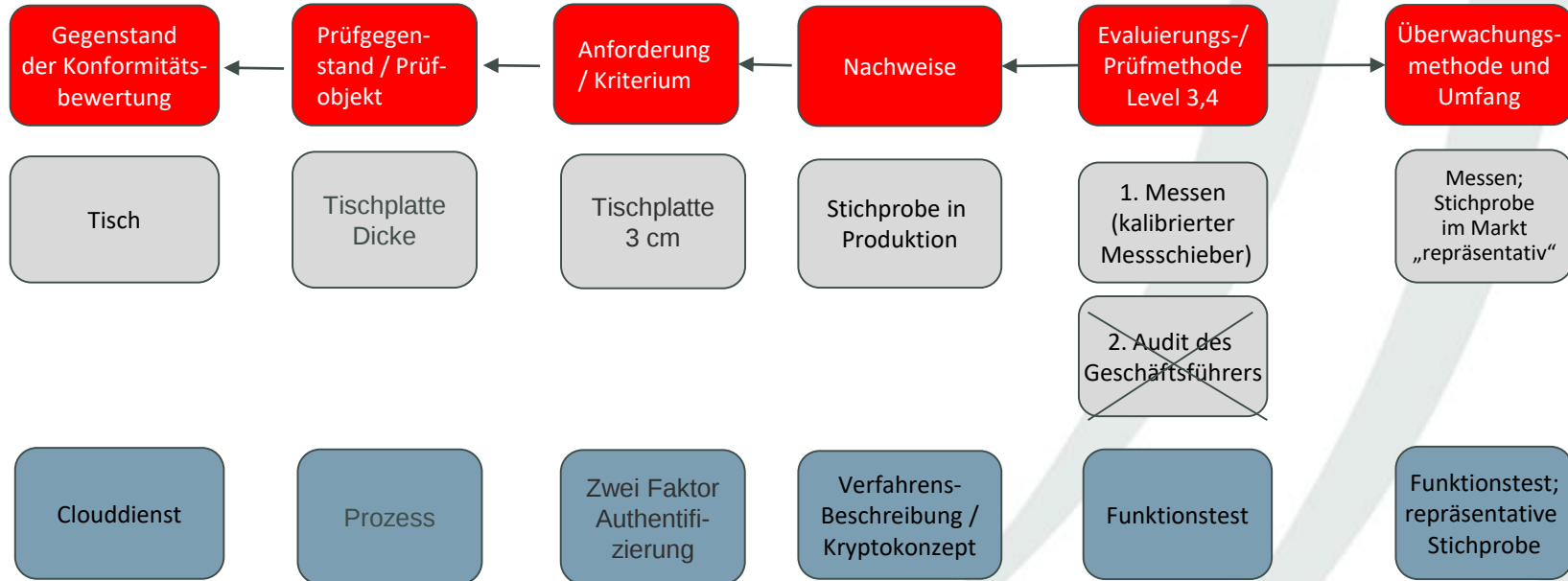
Zertifizierungskriterien

- Beschreiben die Anforderungen der DS-GVO an den Zertifizierungsgegenstand
- Werden von der Aufsichtsbehörde genehmigt

Zertifizierungsprogramm

- Beschreibt den Zertifizierungsmechanismus
- Prüft die DAkkS auf Konformität mit ISO Normen

Der wichtigste Inhalt eines Zertifizierungsprogramms

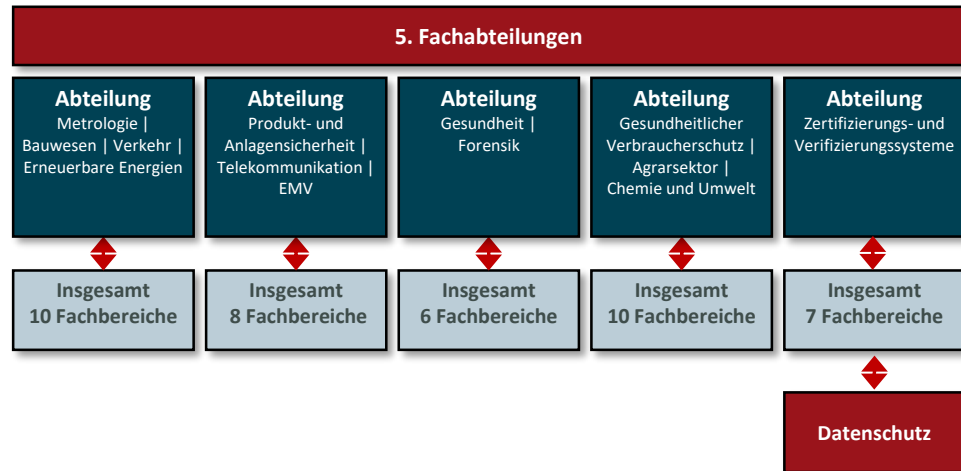


Vielen Dank!

Sie können jetzt mit Fragen löchern!



Ansprechpartner Datenschutz in der DAkkS



Ina Stubenrauch
Abteilungsleitung Zertifizierungs- und Verifizierungssysteme
Ansprechpartner Datenschutz:
Dr. iur. Ilona Pawlowska L.L.M.
ilona.pawlowska@dakks.de