TeleTrusT-Konferenz 2021

Akkreditierung von Zertifizierungsstellen nach DSGVO

Ing. Prof. Dr. iur. Raoul Kirmes M.Sc. (Information Security/Forensik)
Leiter Stabsbereich Grundsatzaufgaben | Deutsche Akkreditierungsstelle

DAkkS
Deutsche
Akkreditierungsstelle

Übersicht

1. DAkkS = Nationale Akkreditierungsbehörde
2. Rechtsrahmen der Datenschutzzertifizierung
3. Anforderungen an die Akkreditierung
4. Status der bisher in Deutschland beantragten Programme
5. Herausforderungen für Verantwortliche/Auftragsverarbeiter

1. DAkkS = Nationale Akkreditierungsbehörde

DAkkS = Nationale Akkreditierungsbehörde

Hoheitliche Aufgabe

- **Einzige nationale** Akkreditierungsbehörde in Deutschland mit **europäischer und internationaler Anerkennung**
- **Sicherstellung hoher Qualität aller Konformitätsbewertungsleistungen**
- **Laufende Überwachung** der **fachlichen Kompetenz** und **Unabhängigkeit** der Konformitätsbewertungsstellen
- **Abbau von Handelshemmnissen** durch Abschluss von **internationalen Gegenseitigkeitsverträgen** für Konformitätsbewertungsergebnisse im Handel mit **Drittstaaten**

DAkkS = Nationale Akkreditierungsbehörde

Nationale Zuständigkeitskonzentration

Art. 4 VO (EG) Nr. 765/2008

„Jeder Mitgliedstaat benennt **eine einzige nationale Akkreditierungsstelle**."

§1 Abs. 1 AkkStelleG

Die Akkreditierung wird als hoheitliche **Aufgabe des Bundes durch die Akkreditierungsstelle** durchgeführt. Diese ist nationale Akkreditierungsstelle im Sinne der Verordnung (EG) Nr. 765/2008 und **für Akkreditierungen nach Artikel 3 der Verordnung (EG) Nr. 765/2008 zuständig** (freiwilliger und gesetzlich geregelter Bereich).

§1 Abs. 1 AkkStelleGBV

Die **Deutsche Akkreditierungsstelle GmbH** wird mit den Aufgaben der nationalen Akkreditierungsstelle nach dem Akkreditierungsstellengesetz beliehen (Beliehene).

DAkkS = Nationale Akkreditierungsbehörde

Abgrenzung: Akkreditierung vs. Zertifizierung

Beispiele für Konformitätsbewertungsstellen

2. Rechtsrahmen der Datenschutzzertifizierung

Im EU-Recht Verweis auf „New Legislative Framework“

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

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.

* Option nur möglich für Mitgliedsstaaten die gemäß Art. 4 Abs. VO (EG)765/2008 keine Akkreditierungsstelle eingerichtet haben.

39 BDSG (Akkreditierung)

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.

Erlaubnis zur Zertifizierung nach DSGVO setzt zwei Verwaltungsverfahren voraus!

Bewährtes 2-Stufen-System

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

1. Stufe:
Akkreditierung durch DAkkS
Kompetenzfeststellung
(„**fachliches Können**“)

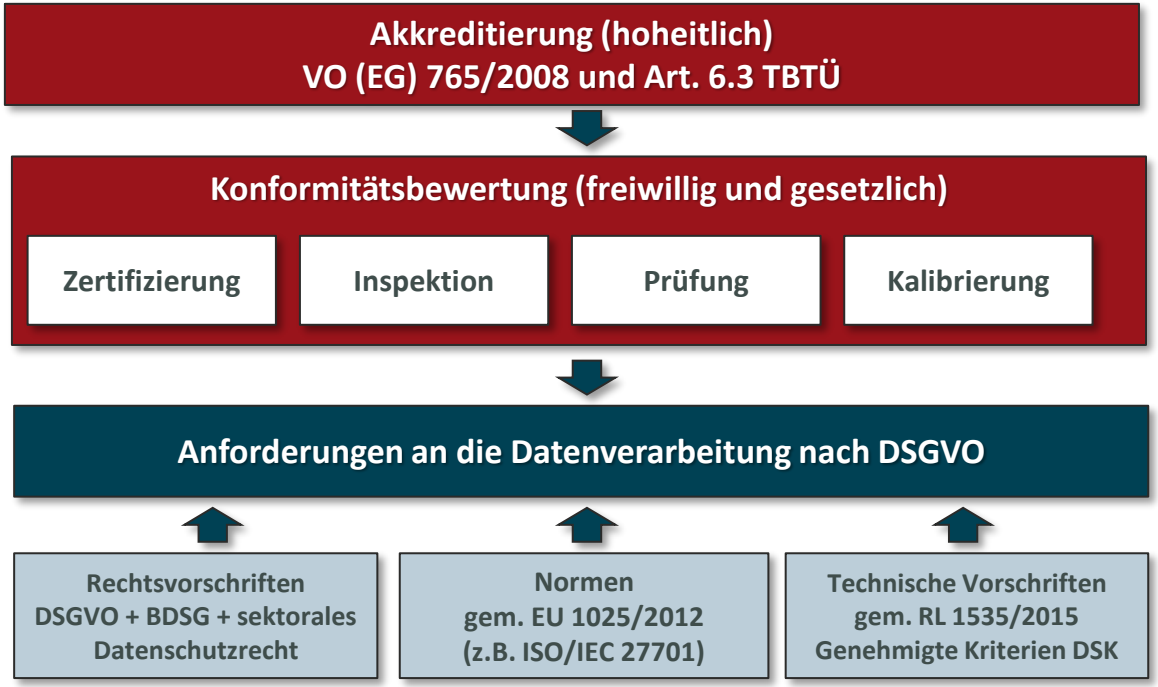
2. Stufe:
Befugniserteilung durch Datenschutz-behörde
Erlaubnis
(„**rechtliches Dürfen**“)

Tätigkeit der KBS
=
Jede Art der
Konformitätsaussage
zu den Anforderungen
der -DSGVO

3. Anforderungen an die Akkreditierung

Horizontale Qualitätsinfrastruktur

Akkreditierung im 3 Ebenen System der Konformitätsbewertung

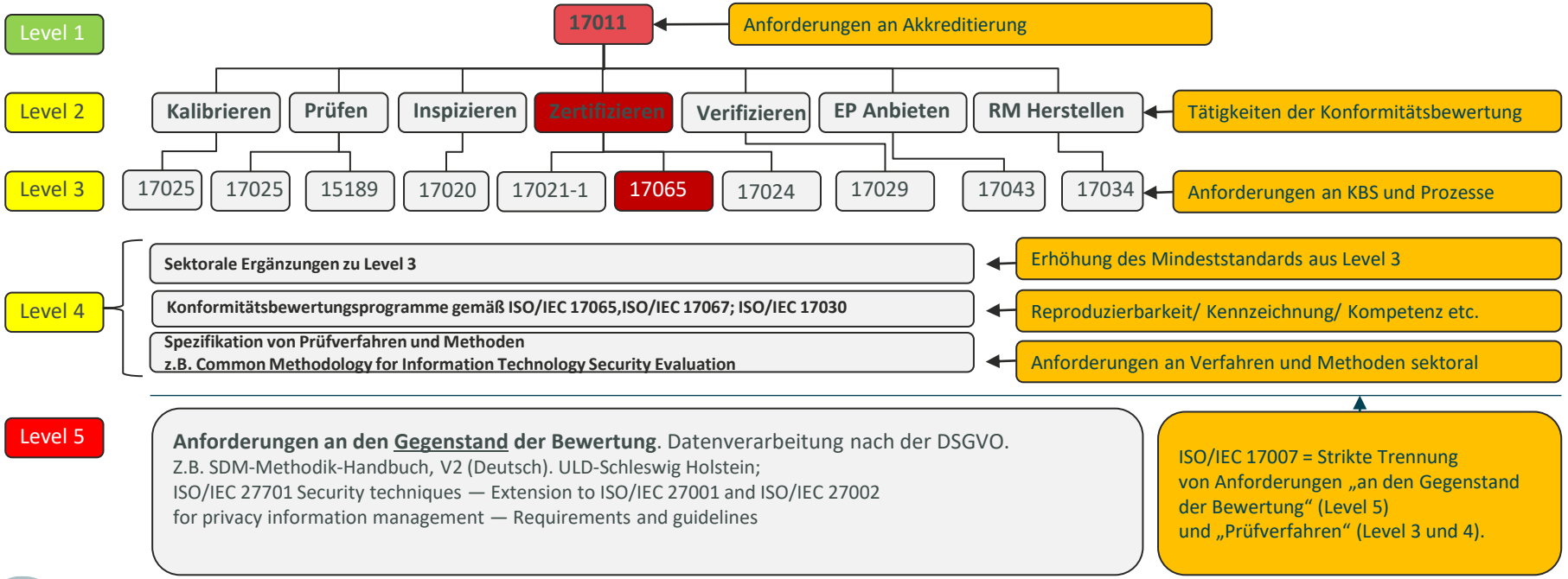


Horizontaler Rechtsrahmen der Akkreditierung

Intern. Ebene	Europäische Ebene	Nationale Ebene
Technical Barriers to Trade Agreement (TBT)	Verordnung (EG) Nr. 765/2008	Akkreditierungsstellengesetz (AkkStelleG)
ILAC MRA/MLA	Verordnung (EU) 2019/515	Beleihungsverordnung (AkkStelleGBV)
IAF-MRA	Beschluss (EG) Nr. 768/2008	Gebührenverordnung
Div. Gegenseitigkeitsabkommen (z.B. CETA, Korea etc.)	Verordnung (EU) Nr. 1025/2012	Akkreditierungssymbolverordnung (SymbolVO)
	Informationsrichtlinie 1535/2015 EU	
	Vergaberichtlinie Art. 44 2014/24/EU	

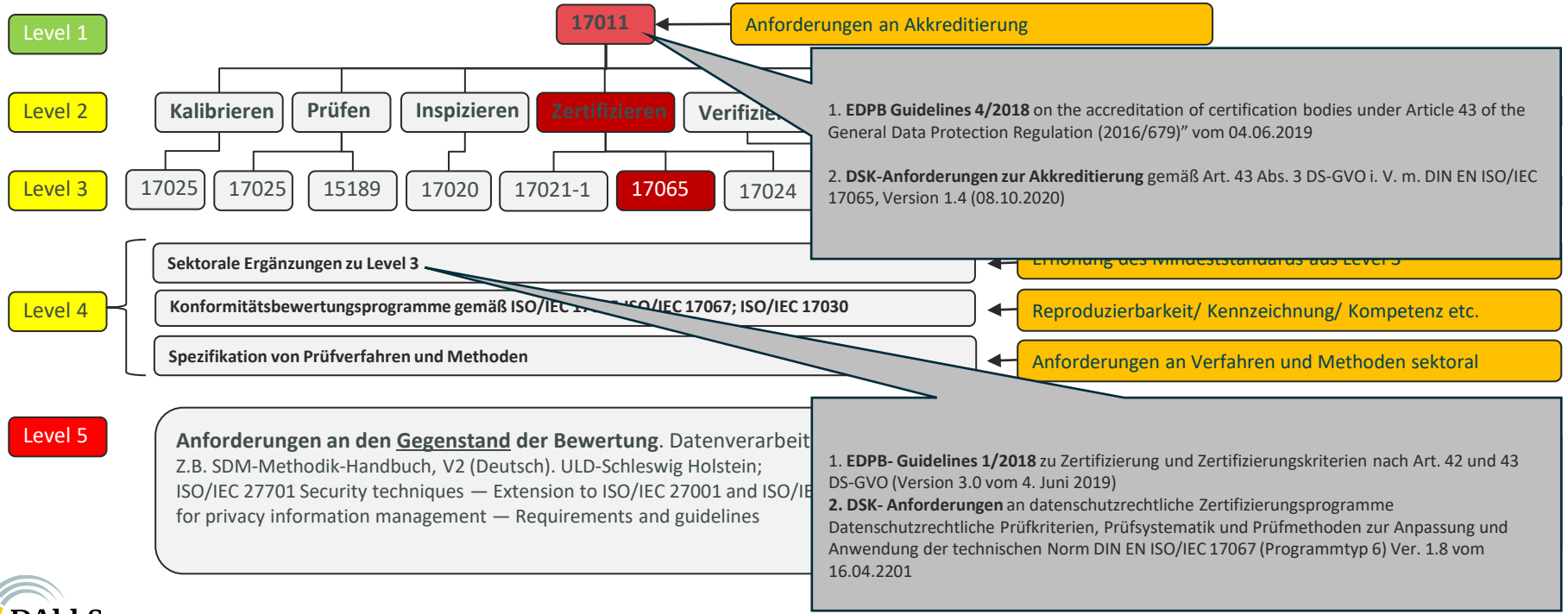
Horizontale Qualitätsinfrastruktur

Normungssystem der Akkreditierung



Horizontale Qualitätsinfrastruktur

Normungssystem der Akkreditierung



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.“

= **Rechtssicherheit für Verantwortliche**, weil in der Zertifizierung der Stand der Technik verbindlich für den Zertifizierungsgegenstand konkretisiert wird.
Die Konformitätsvermutung schließt zwar Bußgelder nicht rechtlich aus, aber praktisch schon, denn eine Sorgfaltspflichtverletzung wird i.d.R. nicht mehr nachweisbar sein.

Genehmigte Programmkriterien nach Art. 42 Abs. 5 DSGVO

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**.

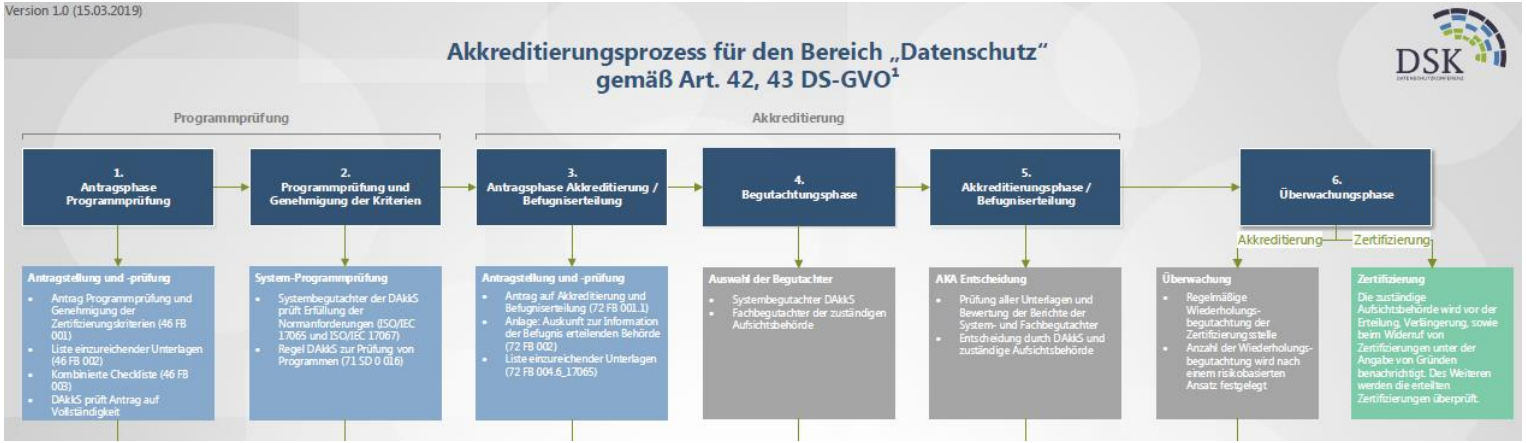
2. Die DAkkS stellt zunächst fest, ob das Konformitätsbewertungsprogramm die Anforderungen der ISO/IEC 17000 Anhang A, ISO/IEC 17007, ISO/IEC 17065 und 17067, 17030 usw. (vgl. **DAkkS-Regel 71 SD 0 016)** erfüllt, um in der Akkreditierung eingesetzt zu werden (Feststellung der Akkreditierungsfähigkeit 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.

Schritt für Schritt zur akkreditierten Zertifizierungsstelle

Weiterführenden Hinweise:

- **DSK-DAkkS-Übersicht zum Akkreditierungsprozess für den Bereich „Datenschutz“ gemäß Art. 42, 43 DS-GVO**
- **DAkkS-Merkblatt zu Akkreditierungsverfahren im Datenschutz vom 25.10.2021**



Horizontale Qualitätsinfrastruktur

Verfügbarkeit von Normen auf Level 5

- SDM-Methodik-Handbuch, V2 (Deutsch). ULD-Schleswig Holstein
- ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 29100 Information technology — Security techniques — Privacy framework
- ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29151 Information technology — Security techniques — Code of practice for personally identifiable information protection
- DIN SPEC 27557 European Cloud Service Data Protection Controls Catalogue

und viele mehr auf sektroaler Ebene (z. BDigitale Gesundheitsanwendungen (DiGA)

4. Status der bisher in Deutschland beantragten Programme

Stand der Programmprüfung in Deutschland

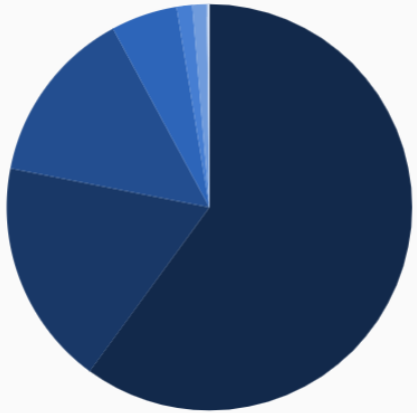
Anzahl der eingereichten Anträge

Nr.	zuständige Aufsichts-behörde (BeB)	Inhalt der Programme	PO / PO und KBS	Status Bearbeitung	
				DAkkS System-prüfung	BeB Fachprüfung
1.	Bremen	Konformitätsbewertungsprogramm zur Zertifizierung von Datenverarbeitungsvorgängen gem. EU-DSGVO	PO und KBS	✓	●
2.	Hamburg	Konformitätsbewertungsprogramm für digitale Produkte und Services nach der DSGVO	PO und KBS	✓	●
3.	NRW	Zertifizierung des gesamten Lebenszyklusses personenbezogener Kundendaten in Deutschland tätiger eCommerce-Unternehmen	PO und KBS	●	
4.	NRW	Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern gemäß DSGVO	PO und KBS	✓	✓
5.	Hessen	DSGVO Zertifizierungsprogramm gemäß Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065	PO und KBS	✓	●
6.	NRW	European Data Protection Certification (AUDITOR) Cloud-Systeme	PO	✓	●
7.	Baden Würtemberg	Automobilunternehmen im Bereich der E-Mobilität	PO und KBS	✓	●
8.	NRW	Management von Datenschutzvorfällen	PO und KBS	●	
9.	Berlin	Nachweis der DSGVO-Konformität von statistischen Auslastungsprognosen und typisierten Interessenprofilen	PO	✓	●
10.	NRW	Zertifizierung von Datenverarbeitungsvorgängen ge. EU-DSGVO	KBS	✓	●
11.	Berlin	Auftragsverarbeitung DSGVO	PO	●	

5. Herausforderungen für Verantwortliche/Auftragsverarbeiter

Problemfelder in Bußgeldverfahren EU-Weit

1. Nach Gesamtsumme der Geldbußen:

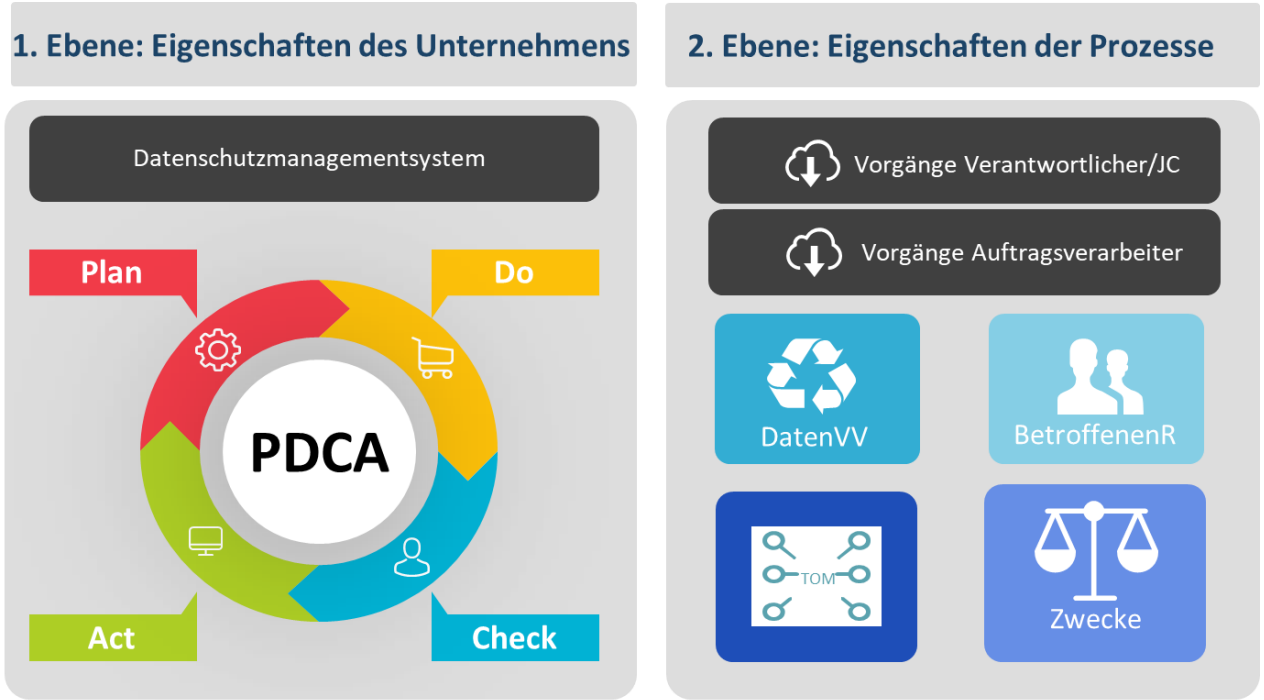


Verstoß	Summe der Geldstrafen
Nichteinhaltung der allgemeinen Grundsätze der Datenverarbeitung	**€ 782.648.664** (bei 178 Bußgeldern)
Unzureichende Erfüllung von Informationspflichten	**€ 234.949.395** (bei 63 Bußgeldern)
Unzureichende Rechtsgrundlage für die Datenverarbeitung	**€ 182.997.138** (bei 299 Bußgeldern)
Unzureichende technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit	**68.993.519 €** (bei 181 Bußgeldern)
Unzureichende Erfüllung von Betroffenenrechten	**16.321.825 €** (bei 79 Bußgeldern)
Unbekannt	**14.700.500 €** (bei 4 Bußgeldern)
Unzureichende Erfüllung der Meldepflichten bei Datenschutzverletzungen	**1.362.091 €** (bei 21 Bußgeldern)
Unzureichende Datenverarbeitungsvereinbarung	**€ 993.580** (bei 5 Bußgeldern)
Unzureichende Einbindung des Datenschutzbeauftragten	**260.200 €** (bei 10 Bußgeldern)
Unzureichende Zusammenarbeit mit Aufsichtsbehörde	**216.929 €** (bei 35 Bußgeldern)

Quelle: CMS https://www.enforcementtracker.com/#

Herausforderungen für Zertifizierungsprozess

Prozesszertifizierung ist anspruchsvoll



DAkkS Deutsche Akkreditierungsstelle

Vielen Dank!

Sie können jetzt mit Fragen löchern!

Ist ein DVV für die Prüfung hinreichend?

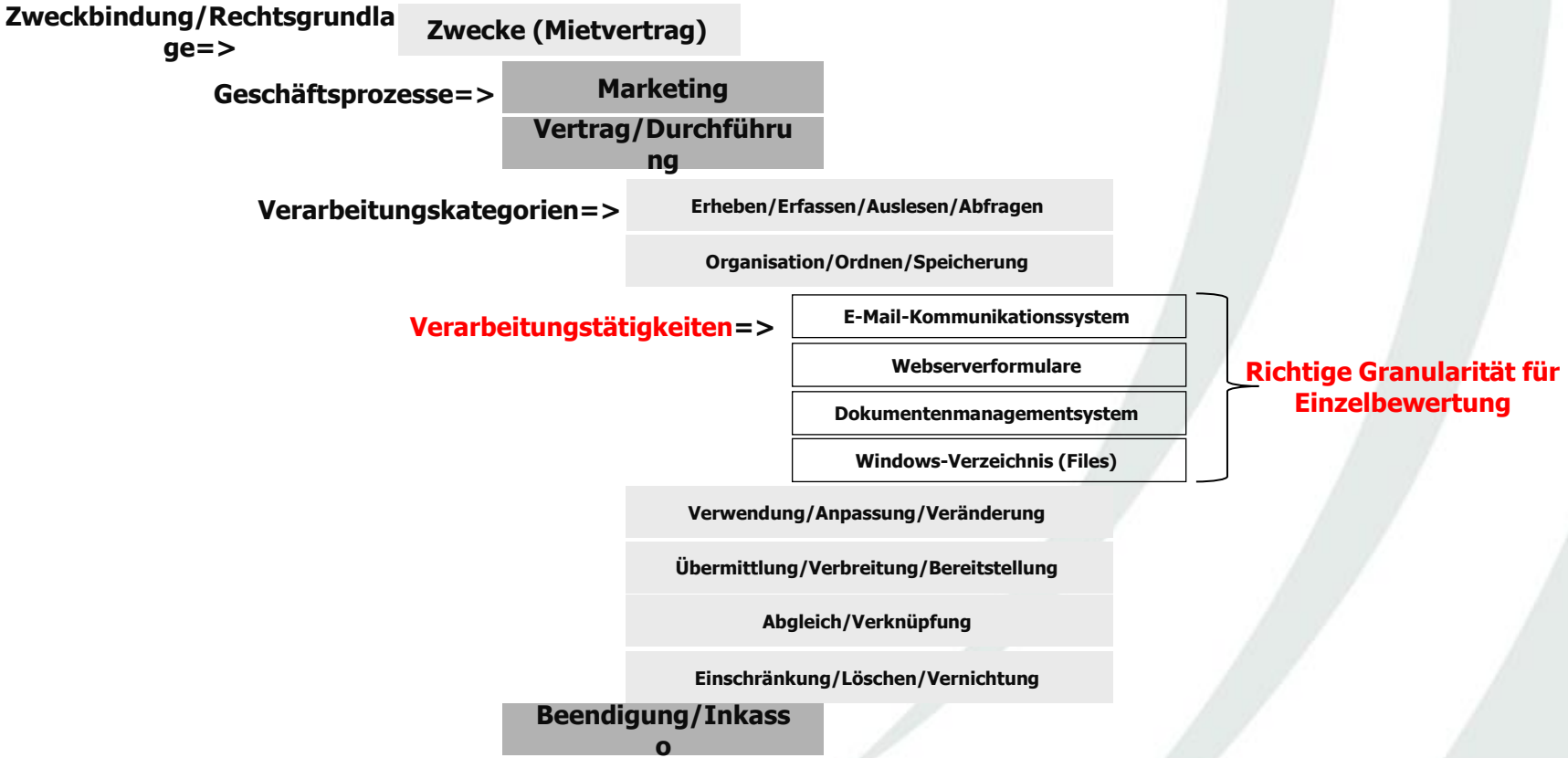
1. Verarbeitungstätigkeiten **als Verantwortlicher** gem. Art. 30 Abs. 1 DSGVO

2. **Ausgelagerte** Verarbeitungstätigkeiten **an Auftragsverarbeiter** gem. Art. 28 DSGVO

3. Verarbeitungstätigkeiten **im Auftrag** als **Dienstleistung** gem. Art 30 Abs. 2 DSGVO

4. **Gemeinsame Verarbeitungstätigkeiten** gem. Art 26 DSGVO

Hauptursache falsche Modellierung der DVV



Probleme der DV-Inventur

Zweckbindung/Rechtsgrundlage=> **Zwecke (Mietvertrag)**

Geschäftsprozesse=> **Marketing**

Vertrag/Durchführung

Verarbeitungskategorien=> **Erheben/Erfassen/Auslesen/Abfragen**

Organisation/Ordnen/Speicherung

Verarbeitungstätigkeiten=> **E-Mail-Kommunikationssystem**

Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c) Beschäftigte Interessenten Lieferanten Kunden Patienten	Kategorien personenbezogener Daten Art. 9 Daten (ja /nein)	Kategorien von Empfängern Intern Extern Drittland	DSF nötig? (ja/nein) geeignete Garantien Nötig ? (ja/nein)	Speicher Dauer 3 Jahre + 1 Monat (Verweis: Löschkonzept)	Anwendung MS- Exchange	Speicherort RZ-1 Berlin	Risikoklasse/ Schutzklasse (normal/erhöht) Verweis auf Risk-M	Referenz TOM´s - - - -	Zugriffs-berechtigte Ggf. Rolle (Verweis BerechtigungsK ZugangsK)	Auslagerung Auftragsverarbeiter/ Joint-Controlling	Rechtsgrundlage der Verarbeitung Art. DSGVO § Spez. Gesetz

Webserverformulare

Dokumentenmanagementsystem

Windows-Verzeichnis (Files)