



ePrivacy  
*European seal for your privacy*

WEBINAR

# Datenschutzzertifikate nach Art. 42 DSGVO

## aktueller Überblick und Einsatzmöglichkeiten

2. Juli 2024

Prof. Dr. Christoph Bauer  
CEO ePrivacy



# Zielsetzung und Themen

1. Zertifizierungen in der DSGVO
2. Prinzipien von Datenschutz-Zertifikaten nach Art. 42 DSGVO
3. Akkreditierung nach Art. 43 DSGVO
4. Zertifizierung nach Art. 42 DSGVO
5. Einsatzmöglichkeiten und Grenzen
6. Alternative: sogenannte „freie“ Siegel
7. Diskussion



# 1. Zertifizierungen in der DSGVO

Art. 42 (1) DSGVO

„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.“

Art. 42 (5) DSGVO

„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 oder – gemäß Artikel 63– durch den Ausschuss genehmigten Kriterien erteilt.“

Art. 42 (7) DSGVO

„Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt ...“

Art. 43 DSGVO

Akkreditierungsverfahren

EG 100

„.....Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das **Datenschutzniveau einschlägiger Produkte und Dienstleistungen** ermöglichen.“

## 2. Prinzipien von Datenschutz-Zertifikaten nach Art. 42 DSGVO

Die Erfüllung grundlegender Prinzipien für Siegel bzw. Zertifikate werden auch für Datenschutz-Zertifikate nach Art. 42 DSGVO verlangt:

1. Öffentlich verfügbarer Kriterienkatalog
2. Auf der Basis von Normen bzw. definierten Anforderungen (i.d.R. EU DSGVO, aber auch BSI-Anforderungen, Stand der Technik etc.)
3. Transparenz des Verfahrens
4. Trennung Beratung – Zertifizierung
5. Qualifizierte und anerkannte Gutachter / Auditoren
6. Veröffentlichung der Zertifikate (inkl. Begründung)
7. Betrieb einer Beschwerdestelle



Audit



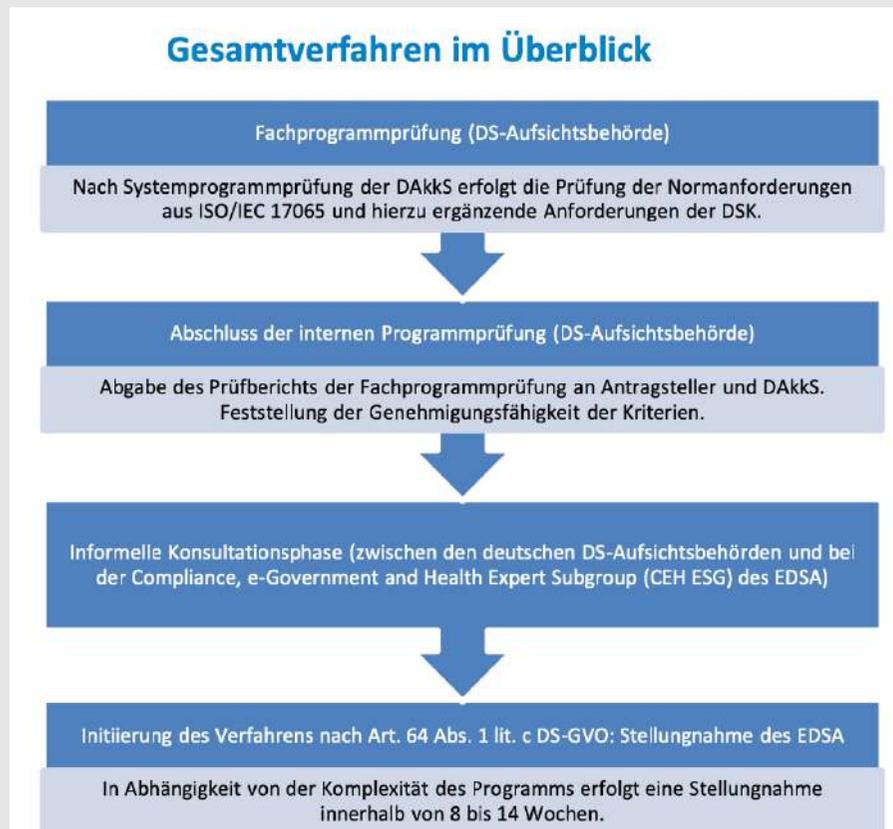
Technische Bewertung



Rechtliche Bewertung

### 3. Akkreditierung nach Art. 43 DSGVO

1. Schritt: Akkreditierung eines Konformitätsbewertungsprogramms sehr komplex / sehr viele Behörden beteiligt



Aus: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Namensnennung – Version 2.0 ([www.govdata.de/dl-de/by-2-0](http://www.govdata.de/dl-de/by-2-0)) DSK, Kurzpapier Nr. 9, Zertifizierung nach Art. 42 DS-GVO, 17.4.23, S. 2

# 3. Akkreditierung nach Art. 43 DSGVO

2. Schritt: Akkreditierung einer Zertifizierungsstelle für ein Datenschutz-Zertifikat ebenfalls sehr aufwändig und langwierig

	<b>Liste einzureichender Unterlagen für die Akkreditierung als Zertifizierungsstelle nach DIN EN ISO/IEC 17065</b>	<b>LI-EU ZE</b>	
		Revision:	<b>1.2</b>
		Datum:	<b>28.01.2022</b>
		Seite:	<b>1/4</b>

Wesentliche Anforderungen (Auszug)

- Unabhängige Zertifizierungsgesellschaft mit aktivem Managementsystem nach ISO17065
- Detaillierte Festlegung aller Unternehmensprozesse nach Verantwortlichkeiten, gelenkten Dokumenten im Managementsystem (Musterformulare für jeden Entscheidungsprozess)
- Absolutes Beratungsverbot für die Gesellschaft
- Beratungsverbot für den Zertifizierungsstellenleiter und die Bewerter und Entscheider, aber sehr umfangreiche Erfahrung im Bereich Datenschutz-Recht und –Technik erforderlich
- Mindestens 6 fest angestellte Evaluatoren für Antragsbewertung, Entscheidung / Bewertung der Evaluation, Beschwerdeverfahren, jeweils für Recht und Technik)
- Begutachtung der Zertifizierungsstelle (2 Tage durch DAkKS und Datenschutz-Behörde)
- etc.

- 01\_Dokumentation Managementsystem
- 02\_Gelenkte Dokumente im Managementsystem
- 03\_Letzte Managementbewertung
- 04\_Aufbau\_Besitz\_Rechtsform
- 05\_Haftung\_Versicherung
- 06\_Mitarbeiter
- 07\_Auftragnehmer
- 08\_AGB + Muster-Verträge
- 09\_Zeichennutzung
- 10\_Geschäftsordnungen\_Gremien
- 11\_Erklärung-Unparteilichkeit
- 12\_Analyse-Unparteilichkeit
- 13\_Verzeichnis\_Zertifikate
- 14\_Zertifikate nach Ländern
- 15\_Liste Länder mit Standort
- 16\_Regeln Ausland + Remote
- 17\_Muster-Zertifikate
- 18\_Zertifizierungsregeln, -programme + Programmprüfung
- 19\_Gebührenordnung\_Preisliste
- 20\_Liste Auditoren
- 21\_Liste Mitarbeiter remote
- 22\_IT-Systeme
- 23\_Teil-Begutachtungsbericht\_Checkliste 17065
- 25\_Unbedenklichkeitsbescheinigungen
- 26\_Liste Prüf-, Kalibrier-, Untersuchungsverfahren
- 27\_Liste Referenzmaterialien zu 26
- 28\_Liste-Teilnahme Eignungsprüfungen
- 29\_Metrologische Rückführung\_Geräteliste
- 30\_Raumplan
- 31\_Teil-Begutachtungsbericht\_Checkliste 17025 bzw. 15189

### 3. Akkreditierung nach Art. 43 DSGVO

Beispiel-Prozess zeigt sehr zeitaufwändigen Akkreditierungsprozess (> 6 Jahre)

Mai 2016 DSGVO tritt in Kraft

Mai 2018 DSGVO-Einführung, Ende der Übergangsfrist

**Jan 2019 erste Antragstellungen auf staatlich akkreditiertes Datenschutz-Siegel möglich**

Dez 2020 DAkkS-Beschluss der Genehmigung eines KBP

Juli 2021 finale fachliche Bewertung der zuständigen Datenschutz-Behörde für das KBP

**Juni 2022 zuständige Datenschutz-Behörde bestätigt DAkkS-Beschluss** (= konformes Programm für ein Datenschutz-Siegel)

Aug 2022 Unterlagen für EDSA-Stellungnahme werden vorgelegt (Vor-Phase)

Okt 2022 Beschluss des Programmausschusses der DAkkS zum KBP (Auflagen, Einschränkung)

**Feb 2023 Bestätigung der DAkkS: alle Auflagen vom Programmausschuss erfüllt, aber eine Einschränkung**

EDSA-Stellungnahme-Verfahren (Vorphase, formale Phase)

2021 Antrag auf Akkreditierung einer Zertifizierungsstelle (DAkkS)

2023 Vor-Ort-Prüfung der Zertifizierungsstelle durch DAkkS und Datenschutz-Behörde

...

Jun 2024 aktueller Stand – siehe folgende Seiten



### 3. Akkreditierung nach Art. 43 DSGVO

Bei der EDSA bisher nur 5 Zertifizierungsprogramme gelistet, davon haben bisher nur 2 Scheme Owner über eine Zertifizierungsstelle ein Siegel verleihen können:

#### Register of certification mechanisms, seals and marks

Name of the scheme	Scheme owner	Competent SA	Certification as tool for transfers	Type of criteria	
Europrivacy	European Centre for Certification and Privacy (ECCP)	LU	No	EU Data Protection Seal	<a href="#">Read more</a>
GDPR-CARPA	LU	LU	No	National certification criteria	<a href="#">Read more</a>
EuroPriSe	EuroPriSe Cert GmbH	DE/LDI NRW	No	National certification criteria	<a href="#">Read more</a>
BC5701:2023	Brand Compliance B.V.	NL	No	National certification criteria	<a href="#">Read more</a>
AUDITOR conformity assessment	Competence Centre Trusted Cloud e.V.	DE/LDI NRW	No	National certification criteria	<a href="#">Read more</a>

EDSA: [https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks\\_en](https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en) v. 25.6.24



# 3. Akkreditierung nach Art. 43 DSGVO

- Europrivacy - verliehenes Zertifikat vollständig?
- Kriterienkatalog öffentlich?

Welcome to the Europrivacy Registry of Certificates managed by the European Centre for Certification and Privacy. In order to search for a certificate, you must fill at least one field (with at least three characters). For more information on Europrivacy certification, feel free to visit [europrivacy.com](https://europrivacy.com).

**Applicant name** 
**Certified object**

**Certification code**

**Created**

**From**  **To**

**Initial date (first certification)**  **Expiration date**

**Certification category**  **Certification status**

**Certification scope**

**Search**

Items per page: 10

Total: 1

Applicant	Certified object	Certification category	Status	More Detail
PricewaterhouseCoopers PWC Luxemburg	"Personal data processing" by eCS (electronic Collaborative Solution)	Process	Approved	

<https://www.europrivacy.org/en/resource/registry> v. 20.6.24

### Certificate details

**Certified object** "Personal data processing" by eCS (electronic Collaborative Solution)

**Certification code** 00A6:A057:A013:0011

**Certified object description** Facilitate secure interactions and the exchange of confidential documents and personal data between PwC Luxembourg and its clients using the eCS (electronic Collaborative Solution)

**Category** Process

**Certification scope** "Personal data processing" by eCS (electronic Collaborative Solution)

**Applicant role** Data Controller

**Certification standard** Europrivacy

**Certification version** v77

**Initial date (first certification)** 23 May 2024

**Renewal date (if applicable)** 21 June 2024

**Expiration date** 22 May 2027

**Status** APPROVED

**DP ID URL (if available)**

**Evaluation methods and tests** Remote assessment, online evaluation, documentation review

**Summary of Evaluation results** TAM CERT Hungary Inspection and Certification Ltd. certifies that the Target of Evaluation is complying with the applicable requirements of the Certification Scheme

**Reasons for granting or revoking the certification** The Certificate was issued after the accredited Certification Body fully conducted the conformity assessment procedure according to the Europrivacy GDPR Scheme with regard to the Target of Evaluation, and as a result of the procedure made a positive certification decision on the basis of compliance with the relevant criteria.

**Share this page** Use the following URL: <https://repository.europrivacy.org/en/certificati>

**Public comment (including Scope Modification)** -




### 3. Akkreditierung nach Art. 43 DSGVO

EuroPriSe - Zertifikate nur für Auftragsverarbeiter

- aktuelles Zertifikat vom Dez. 23, im Januar 2024 erst Akkr.urkunde vom LDI NRW erhalten (lt. Presse)

**Zertifikatsliste für Auftragsverarbeiter**  
Genehmigte Zertifikate gemäß Artikel 42 DSGVO, die auf Grundlage des EuroPriSe Zertifizierungsprogramms für Auftragsverarbeiter erteilt wurden („Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern gemäß DSGVO nach der EuroPriSe Methode“).  
Ausführliche Informationen zu den einzelnen Zertifizierungen finden Sie, wenn Sie auf den Link unter „Short Report“ klicken.

**2024**

Antragsteller	Zertifizierungsgegenstand	Gültigkeit	Short Report	Zertifikat
RISER ID Services GmbH	RISER-Service	18. Dezember 2026		EPS-AV-20240001

 **Über EuroPriSe**  
Zertifizierungsprogramm  
Zertifikatslisten

**Kontakt**  
Joseph-Schumpeter-Allee 25  
53227 Bonn

<https://euprivacyseal.com/de/europrise-zertifikatslisten/> v. 25.6.24



## 3. Akkreditierung nach Art. 43 DSGVO

BrandCompliance - Programm bisher nicht öffentlich frei verfügbar?  
- in Deutschland so akkreditierbar?



The screenshot shows the BrandCompliance website interface. At the top left is the logo 'BC Brand Compliance'. To its right is a button 'VRAAG EEN OFFERTE AAN' and a search bar with the text 'Zoek...'. Below the logo is a navigation menu with items: 'Informatiebeveiliging', 'Privacy', 'Kwaliteit', 'Kennisbank', 'Nieuws', 'Academy', and 'Over ons'. The main content area has a breadcrumb trail: 'Home / BC 5701 / AVG Certificeringsstandaard en -criteria BC 5701:2023 (NL)'. The product title is 'AVG Certificeringsstandaard en -criteria BC 5701:2023 (NL)'. Below the title is the price '€245.00 excl. btw'. A list of specifications follows: 'Aantal pagina's: 181', 'Vorm: Digitaal PDF bestand (per e-mail verzonden)', 'Datum van publicatie: 23-10-2023', 'Taal: Nederlands', and 'Titel: AVG Certificeringsstandaard en -criteria BC 5701:2023 (NL)'. To the left of the text is an image of a PDF document with a red 'PDF' icon overlaid. Below the specifications is a paragraph of text: 'AVG Certificeringsstandaard en -criteria BC 5701 (NL) biedt een raamwerk waarmee organisaties op systematische wijze invulling kunnen geven aan de eisen van de AVG/ GDPR en de daarbij horende verantwoordingsplicht. De BC 5701 is toepasbaar voor alle organisaties die de rol van verwerkingsverantwoordelijke en/of verwerker van persoonsgegevens vervullen, ongeacht de omvang of het soort producten/diensten dat wordt geleverd. Na implementatie van de BC 5701 is certificering mogelijk, waarmee organisaties kunnen aantonen aan de eisen te voldoen.'

<https://brandcompliance.com/product/avg-certificeringsstandaard/>



# 3. Akkreditierung nach Art. 43 DSGVO

- DAkKS - akkreditierte Stellen für Datenschutz von Datenschutz Cert und EuroPriSe
- akkreditiertes Programm von AUDITOR (vom LDI NRW)

The screenshot shows the DAkKS website search results for 'Suchergebnis Akkreditierte Stellen'. The search criteria are 'Treffer: 2, Begriff: Datenschutz'. A 'ZURÜCK ZUR SUCHE' button is visible. The results are filtered by 'Status' (Aktiv (2)), 'Art der Konformitätsbewertung' (Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen (2)), 'Bereiche', and 'Rechtsgrundlagen'. Two results are listed: 'datenschutz cert GmbH' and 'EuroPriSe Cert GmbH', each with a 'DETAILINFORMATION' button and a 'GELTUNGSBEREICH PDF | DE' link.

The screenshot shows the DAkKS website program page for 'Programme im Bereich Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen'. The accreditation is for 'DIN EN ISO/IEC 17065'. A specific program is listed: 'DS-GVO | European Data Protection Certification (AUDITOR)'.

<https://www.dakks.de/de/akkreditierte-stellen-suchergebnis.html?page=1> v. 25.6.24



# Anwendungsbereich von Art. 42 Zertifikaten

Der Anwendungsbereich von Datenschutz-Zertifikaten nach Art. 42 DSGVO ist sehr eng:

- nur anwendbar bei konkreten Datenverarbeitungsprozessen
- nicht anwendbar bei Datenschutz-Managementsysteme, White Label-Lösungen, Plattformen, etc.
- Anwendung fraglich, wenn rechtlicher Graubereich betroffen ist (aktuelles Beispiel: consent für PUR-Modelle)
- Grundsätzlich risikobasierter Ansatz in der DSGVO angelegt, aber i.d.R. Extrem-Forderungen der Behörden
- Kein vereinfachtes Verfahren für SME trotz risikobasiertem Ansatz der DSGVO
- für den deutschen / europäischen Markt ausgelegt (i.d.R.)
- bei Datenverarbeitung im EU-Ausland: i.d.R. keine Zertifizierung möglich
- Bei Joint Controller / Independent Controller Modellen: alle Controller müssen zertifiziert werden

# Betrieb einer Zertifizierungsstelle nach Art. 43 DSGVO

## Der Betrieb einer staatlichen anerkannten Zertifizierungsstelle erfordert permanent einen hohen Aufwand

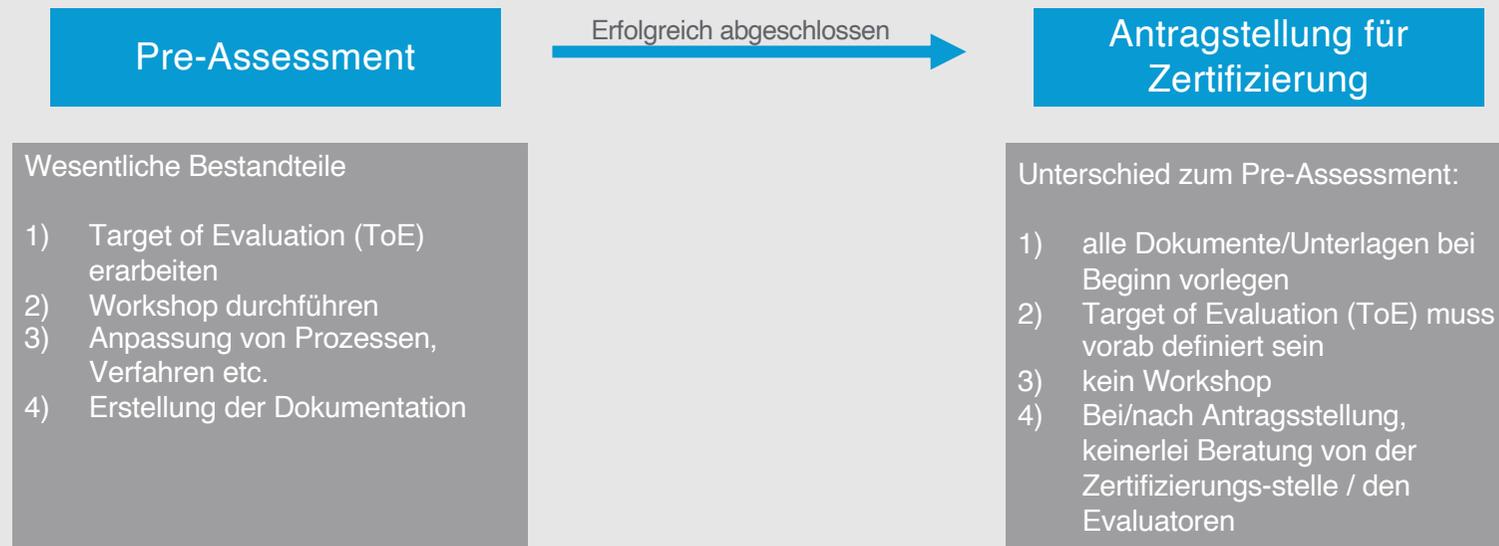
- Ressourcen und Kompetenz der Zertifizierungsstelle
    - Anerkennung von Evaluatoren für Recht und Technik
    - Weiterbildung der Evaluatoren und laufende Kompetenznachweise der Evaluatoren (aktuelles know how)
    - Eine hohe Anzahl von Evaluatoren für Recht und Technik ist für einen laufenden Betrieb erforderlich:
      - Separate Evaluatoren (Recht /Technik) notwendig für 1) Antragsprüfung, Auditplanung, 2) Evaluation, 3) Bewertung der Evaluation und Zertifizier-Entscheidung und 4) mögliche Prüfungen von Beschwerden
      - Für einige der Evaluatoren (für Bewertung/Entscheidung und separate f. mgl. Beschwerden) gilt nach DAkkS-Vorgaben ein absolutes Beratungs-Verbot
  - Laufende Anpassungen des Programms müssen gewährleistet sein
    - an neue Gesetze, Anforderungen der Datenschutz-Behörden, Gerichtsentscheidungen etc.
    - ggf. zusätzliche Genehmigungen von Datenschutz-Behörden und DAkkS erforderlich
  - Weiterentwicklung des Programms (KBP)
    - Erweiterungen für neue Anwendungen: z.B. eHealth generell, DiGA / DiPA – extra-Katalog – BfArM (V1 v. 24.4.24, 79 Seiten\*) ), neue Technologien (AI etc.), exakte Prüfschritte sind festzulegen
    - Vor. Genehmigungen von Datenschutz-Behörden und DAkkS erforderlich
- Der Betrieb einer Zertifizierungsstelle ist sehr personalintensiv und führt zu hohen Kosten für den Zertifizierungsprozess

\*) Achtung: Das Zertifikat befindet sich weiterhin in der Entwicklung. Daher sind weitere Änderungen an den Prüfkriterien möglich.

## 4. Zertifizierung nach Art. 42 DSGVO

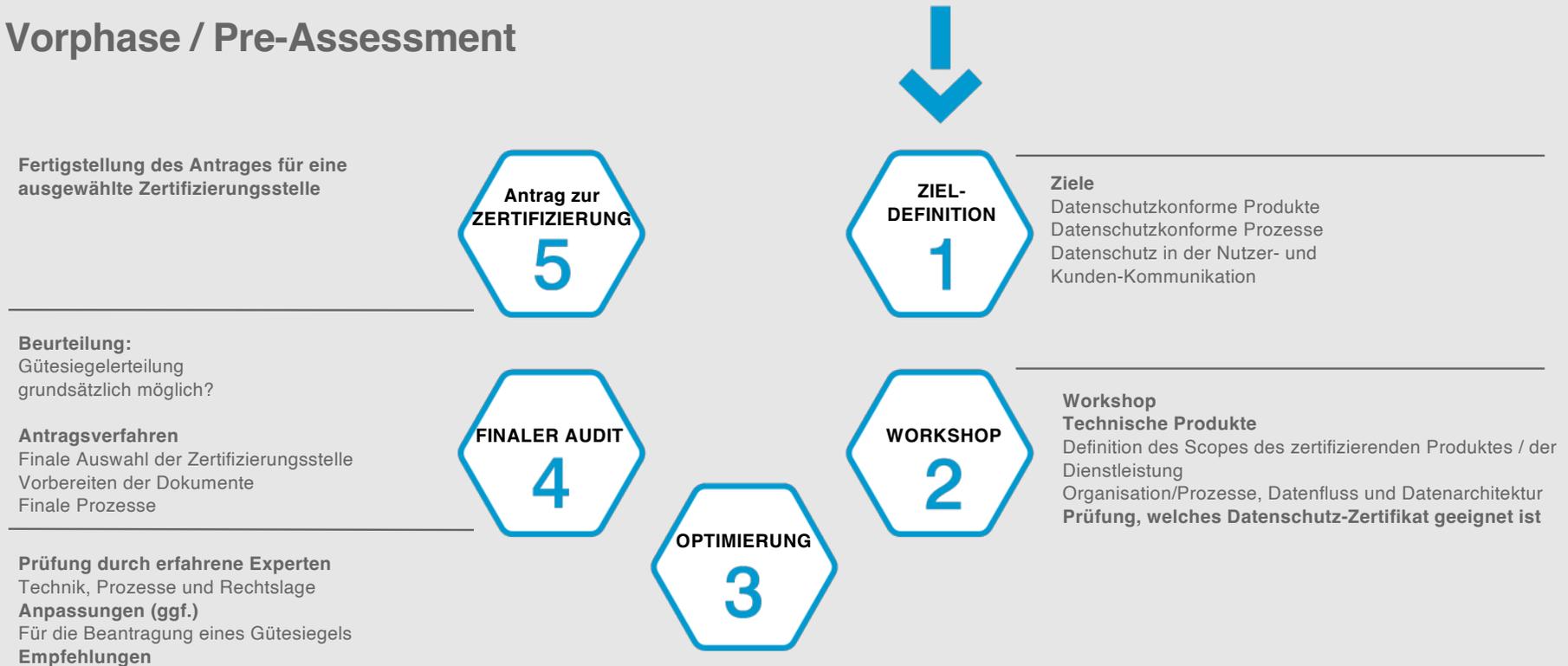
Materielle Voraussetzung für den Zertifizierungsbeginn:

- erfolgreich abgeschlossenes Pre-Assessment (Vor-Prüfung)
- Zertifizierungsgesellschaften und beteiligte Auditoren dürfen nicht beraten!
- Beratung von spezialisierten Beratungsgesellschaften möglich (z.B. ePrivacy GmbH etc.)



# 4. Zertifizierung nach Art. 42 DSGVO

## Vorphase / Pre-Assessment



Ergebnis: Abgeschlossenes Pre-Assessment (ca. 3-6 Monate)

## 4. Zertifizierung nach Art. 42 DSGVO



## 5. Einsatzmöglichkeiten und Grenzen: Vorteile von Art. 42 Zertifikaten

- Zertifikat einer staatlich anerkannten Zertifizierungsstelle hat hohe Anmutung
- Haftungserleichterungen Art. 83 (2) j DSGVO,
- für Auftragsverarbeiter zum Nachweis von Garantien Art. 28 (5) DSGVO einsetzbar
- Dokumentationserfüllung
  - Aber auch : Art. 42 Abs. 4: „ ... Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden bleiben von einer Zertifizierung unberührt.“
- Laufzeit von 3 Jahren

In Summe

- Begrenzte rechtliche Vorteile lt. DSGVO

## 5. Einsatzmöglichkeiten und Grenzen: Nachteile von Art. 42 Zertifikaten

- Enger Anwendungsbereich
- begrenzte rechtliche Vorteile
- Kritischer Punkt: Forderung der Umsetzung aller Empfehlungen von Datenschutz-Behörden („Orientierungshilfen“, Stellungnahmen etc.), auch wenn sie rechtl. nicht zwingend notwendig sind !
- Behörden stimmen sich nicht richtig ab (doppelter Aufwand, ggf. Widersprüche) – was passiert bei unterschiedlichen Ansichten der Behörden?
- Trotz Zertifizierung keine geminderte Verantwortung des Verantwortlichen oder Auftragsverarbeiters für Einhaltung der DSGVO (Art. 42 (4)).
- Hoher Aufwand & Kosten
  1. hoher Aufwand für Siegel-Inhaber bei Aufbau und Bereithalten der Dokumentationen, Prozess-Detaillierung etc.
  2. sehr hoher Aufwand beim Aufbau und Betrieb einer Zertifizierungsstelle
  3. Dokumentationen und Zugang zu Verarbeitungen für zuständige Behörde verfügbar (DSGVO Art. 42 (6))
  4. Hoher interner Personal- / Kostenaufwand inkl. Vor-Phase / Pre-Assessment
  5. hohe Kosten des Siegels (+50-80%)
- hoher Zeitbedarf zur Erlangung eines Siegels (Vor-Phase, ca. 3-6 Monate, Hauptphase mind. 9-12 Monate )

## Zwischenergebnis

Für Interessenten empfiehlt sich ein Datenschutzzertifikat nach Art. 42 nur anzustreben, wenn

**ein solches Siegel gesetzlich vorgeschrieben ist (z.B. bei DiGA /DIPA, was aber noch nicht verfügbar ist)**

oder

**b) der jeweilige Markt ein solches Siegel sehr stark erwartet und andere alternative Lösungen nicht ausreichen.**

## 6. Alternative: sogenannte „freie“ Siegel

„private“ DSGVO-Zertifizierungen/-Siegel, die außerhalb des Anwendungsbereiches der Art. 42, 43 DSGVO liegen, existieren wie bisher und erfreuen sich großer Beliebtheit:

- Detailliertes technisches und rechtliches Datenschutz-Gutachten auf der Basis eines öffentlich verfügbaren Datenschutz-Kriterienkatalogs von erfahrenen und anerkannten technischen und rechtlichen Gutachtern
- Bei positiven Gutachten Bestätigung der Einhaltung des Kriterienkatalogs durch ein „Zertifikat“
- Hinweis aus wettbewerbsrechtlichen Gründen: „Kein genehmigtes Verfahren im Sinne der Art. 42 und 43 DSGVO“

### Erfüllung der genannten grundlegender Prinzipien für freie Siegel bzw. Zertifikate

- Öffentlich verfügbarer Kriterienkatalog
- Auf der Basis von Normen bzw. definierten Anforderungen (i.d.R. EU DSGVO, aber auch BSI-Anforderungen, Stand der Technik etc.)
- Transparenz des Verfahrens
- Trennung Beratung – Zertifizierung
- Qualifizierte und anerkannte Gutachter / Auditoren
- Veröffentlichung der Zertifikate (inkl. Begründung)
- Betrieb einer Beschwerdestelle

## 6. Alternative: sogenannte „freie“ Siegel

### Zulässigkeit freier Siegel

- die Literatur zeigt ganz überwiegende Meinung, dass freiwillige Siegel neben dem staatlichen Siegel stehen können
  - Kein Verbot anderer Siegel in der DSGVO
  - Andere Siegel können auch wertig sein
  - Beispiel-Quellen:
    - „...können Siegel, die nicht Art. 42 DSGVO unterfallen, gleichwohl innovative oder überobligatorische Prüfungsmaßstäbe begründen und aufgrund ihrer leichteren Zugänglichkeit einen größeren Adressatenkreis ansprechen. ...“ \*)
    - „Zertifizierungen können ein wirkungsvolles Instrument sein, um ein Bewusstsein für Datenschutz zu schaffen und den Wettbewerb in Richtung von mehr Datenschutz zu triggern. Diese Wirkung sollte nicht durch ein falsches Verständnis des Art. 42 DSGVO voreilig nur auf die akkreditierten Zertifizierungen beschränkt werden. „ \*)
- \*) Müllmann / Spiecker, in DVBL 4 2022, S. 208 – 214

### Wichtige Rahmenbedingungen für freie Siegel

- wettbewerbsrechtliche Irreführung vermeiden
  - DAkkS und das Wettbewerbsrecht verlangen klare Abgrenzung zu Art. 42 DSGVO
- "Kein genehmigtes Verfahren im Sinne der Art. 42 und 43 DSGVO"

## 6. Alternative: sogenannte „freie“ Siegel

### Vorteile

- Größerer Anwendungsbereich
- Bestätigt auch die Einhaltung des DSGVO
- Keine Abhängigkeit von konkreten Datenverarbeitungen
- Deutlich geringere Kosten, geringerer Zeitaufwand, praktisch derselbe Prüfungsgegenstand
- Unternehmen nutzen freie Siegel für interne Audits
- Schneller (ca. 4-6 Monate) und deutlich kostengünstiger zu erlangen

### Nachteile

- entsprechend den genannten Vorteilen der Datenschutz-Zertifikate nach Art. 42 DSGVO

## 6. Alternative: sogenannte „freie“ Siegel

Beispiele (mit / ohne direkten DSGVO-Bezug)

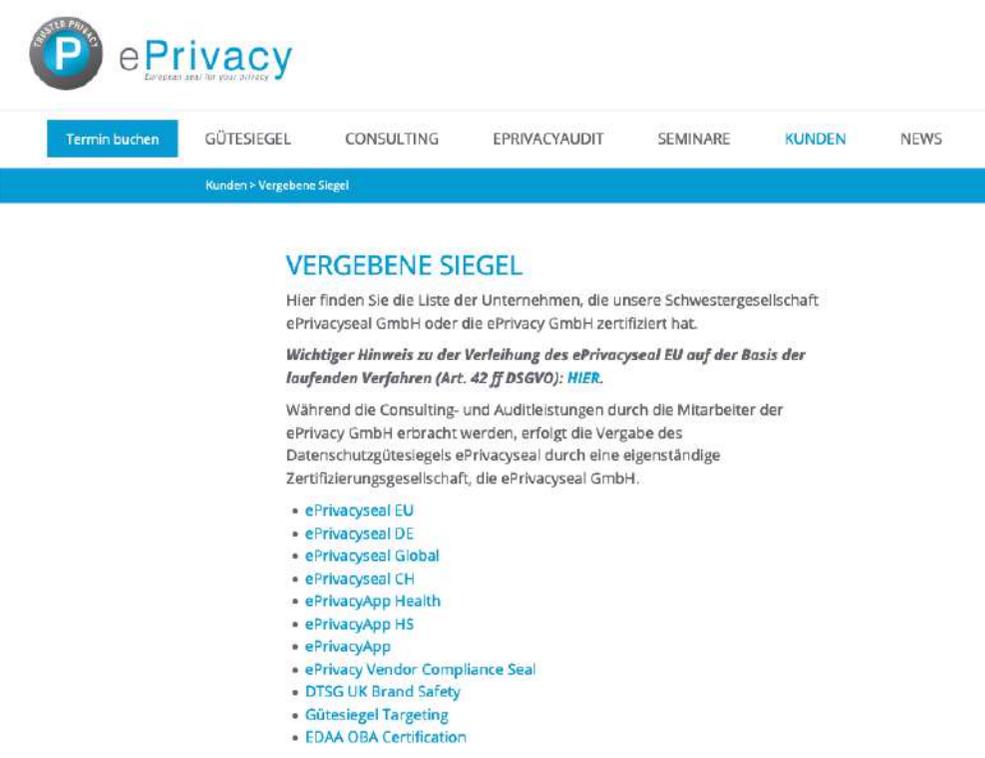
- Zertifizierung eines Datenschutzmanagementsystems (nach ISO27701 oder nach CPS100)  
<https://www.iitr.de/produkte-services/datenschutzmanagementsystem-ck2>
- ePrivacyseal EU (ePrivacy GmbH) <https://www.eprivacy.eu/quetesiegel/eprivacyseal>
- Trusted Site Privacy: Zertifizierung des betrieblichen Datenschutzes  
<https://www.tuvit.de/de/leistungen/datenschutz/datenschutz-zertifizierung/trusted-site-privacy/>
- „Trusted Data Processor“-Zertifizierung für Auftragsverarbeiter (Verhaltensregel gem. Art. 40 DSGVO)  
<https://www.gdd.de/die-gdd/dsz/>
- Personenzertifikate, z.B. Zertifikat als „Datenschutzbeauftragter“, „Datenschutzauditor“, „Externer Datenschutzbeauftragter“, IAPP etc.
- ggf. weitere



## 6. Alternative: sogenannte „freie“ Siegel

### ePrivacy

- Freie Siegel verfügbar für Datenschutz und Datensicherheit
- Kriterienkataloge öffentlich verfügbar
- Keine Beratung durch Auditoren
- Etc.
  
- Über 450 Siegel verliehen (seit 2012)
- Datenschutz-Siegel in 3-5 Monaten erreichbar



The screenshot shows the ePrivacy website interface. At the top left is the ePrivacy logo with the tagline 'European seal for your privacy'. Below the logo is a navigation menu with buttons for 'Termin buchen', 'GÜTESIEGEL', 'CONSULTING', 'EPRIVACYAUDIT', 'SEMINARE', 'KUNDEN', and 'NEWS'. A blue banner below the menu reads 'Kunden > Vergebene Siegel'. The main content area is titled 'VERGEBENE SIEGEL' and contains the following text:

Hier finden Sie die Liste der Unternehmen, die unsere Schwestergesellschaft ePrivacyseal GmbH oder die ePrivacy GmbH zertifiziert hat.

**Wichtiger Hinweis zu der Verleihung des ePrivacyseal EU auf der Basis der laufenden Verfahren (Art. 42 ff DSGVO): [HIER](#).**

Während die Consulting- und Auditleistungen durch die Mitarbeiter der ePrivacy GmbH erbracht werden, erfolgt die Vergabe des Datenschutzgütesiegels ePrivacyseal durch eine eigenständige Zertifizierungsgesellschaft, die ePrivacyseal GmbH.

- ePrivacyseal EU
- ePrivacyseal DE
- ePrivacyseal Global
- ePrivacyseal CH
- ePrivacyApp Health
- ePrivacyApp HS
- ePrivacyApp
- ePrivacy Vendor Compliance Seal
- DTSG UK Brand Safety
- Gütesiegel Targeting
- EDAA OBA Certification

<https://www.eprivacy.eu/kunden/vergebene-siegel> v. 25.6.24



# Fazit

## Datenschutz-Zertifikate nach Art. 42 DSGVO

1. Datenschutz-Zertifikate nach Art. 42 werden demnächst von verschiedenen Zertifizierungsstellen angeboten werden.
2. bei der Auswahl eines Datenschutz-Zertifikates ist der Scope des Zertifikates zu berücksichtigen (Processor, Cloud, DiGA? etc.)
3. einige Einschränkungen: nur konkrete Datenverarbeitungsprozesse können zertifiziert werden etc.
4. Risiken hinsichtlich der Rechtssicherheit der Anforderungen, z.B. Umsetzung aller „Arbeitspapiere“ und weiterer Empfehlungen der Datenschutz-Behörden erforderlich (Stellungnahmen, Orientierungshilfen etc.)
5. es mangelt an einfacheren Lösungen bei „risikoarmer“ Datenverarbeitung und Lösungen für SME und neue Technologien
6. sehr langer und komplexer Prozess der Anerkennung der Zertifikate führt zu einem komplexen und aufwändigen Betrieb der Zertifizierungsstellen und entsprechend hohen Kosten für Antragsteller

## „Freie“ Datenschutz-Siegel als Alternative

1. „freie“ od. „private“ Siegel sind möglich, seit vielen Jahren bewährt und werden umfangreich genutzt
2. als umfassendes Gutachten leisten sie viel mehr, als üblicherweise in Unternehmen dokumentiert wird.
3. als Nachweis für die Einhaltung der DSGVO (außer Art. 42) sinnvoll,
4. für Marketing-Zwecke sehr gut einsetzbar
5. breiterer Anwendungsbereich (auch für Management-Systeme, Plattformen)
6. sinnvoller Einsatzbereich (flexiblere Gestaltung für SME und neue Technologien etc.)
7. deutlich günstigerer und schnellere Zertifizierung



## Diskussion

Prof. Dr. Christoph Bauer  
CEO  
ePrivacy GmbH  
[c.bauer@eprivacy.eu](mailto:c.bauer@eprivacy.eu)

[www.eprivacy.eu](http://www.eprivacy.eu)



ePrivacy

Datenschutz und Datensicherheit für Unternehmen