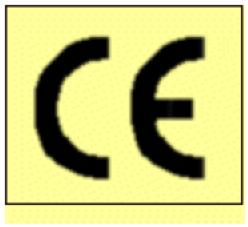
Datenschutz-Zertifizierungen: Neue Möglichkeiten für Unternehmen und Verwaltung

Henry Krasemann

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gütesiegel über Gütesiegel


CE

Zertifizierungen – Sinn und Zweck

- Eigenkontrolle
- Vertrauensbildung (Kunden und Geschäftspartnern gegenüber)
- Werbung

- Ggf. gesetzliche Vorteile (Nachweise / Anfragen Aufsichtsbehörde etc.)

Bis 24. Mai 2018

- Datenschutz-Gütesiegel Schleswig-Holstein
  - Anerkannte Gutachter prüfen Produkte
  - ULD zertifiziert
  - Grundlage: LDSG SH und DSGSVO

- Audit
  - ULD prüft öffentliche Stellen
  - Grundlage: LDSG SH

Seit 25. Mai 2018

- LDSG: Zertifizierungen und Audit gestrichen

- Zertifizierungen nach Artt. 42 / 43 DSGVO
  - durch akkreditierte private Stellen oder
  - durch Aufsichtsbehörden
    - Wenn sie denn wollen

Neue Aufgaben für alle Aufsichtsbehörden nach DSGVO

- Art. 57 DSGVO: „Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet…
  - n) die **Einführung von Datenschutzzertifizierungsmechanismen** und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 **billigen**;
  - o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig **überprüfen**;
  - p) die **Kriterien für die Akkreditierung** einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 abfassen und veröffentlichen;
  - q) die **Akkreditierung** einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Artikel 41 und einer Zertifizierungsstelle gemäß Artikel 43 **vornehmen**;

Und die Befugnisse …

- Art. 58 DSGVO: Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten, …
  - h) eine **Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen**, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden …

Vorteile der Zertifizierung

- Gesichtspunkt für Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3 DSGVO)
- Faktor beim Nachweis der Erfüllung der Anforderungen des Art. 25 Abs. 1 und 2 DSGVO (vgl. Abs. 3)
- Faktor beim Nachweis der Garantien des Auftrags-verarbeiters nach Art. 28 DSGVO (vgl. Abs. 5 und 6)
- Faktor beim Nachweis „Sicherheit der Verarbeitung" (Art. 32 Abs. 3 DSGVO)
- Garantie für Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f DSGVO)

Artt. 42 und 43 DSGVO: Grundstruktur

- Wer kann zertifizieren?
  - Aufsichtsbehörden und akkreditierte Zertifizierungsstellen (Art. 42 Abs. 5 DSGVO)
- Was wird zertifiziert?
  - Dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird (Art. 42 Abs. 1 DSGVO)
    - Beinhaltet Produkte, Verfahren, Prozesse, Dienstleistungen mit konkreter Datenverarbeitung
    - Nicht: Reine Managementsysteme / Konzepte
- Bindung der Aufsichtsbehörden?
  - Nein: Art. 42 Abs. 4 DSGVO

Artt. 42 und 43 DSGVO: Grundstruktur

- Wie wird man (neben den Aufsichtsbehörden) Zertifizierungsstelle? (Voraussetzungen in Art. 43 DSGVO)
  - Akkreditierung durch Aufsichtsbehörde oder nationale Akkreditierungsstelle
    - BDSG-Neu: Deutsche Akkreditierungsstelle GmbH zusammen mit Aufsichtsbehörden (Gutachter/Befugniserteilung)
    - Grundlage: ISO 17065
  - Nachweis von Unabhängigkeit, Fachwissen, keine Interessenskonflikte
  - Genehmigte Kriterien (Konformitätsbewertungsprogr.)
    - Zertifizierungsverfahren erlassen (inkl. Widerruf etc.)
    - Beschwerdeverfahren

Geänderte Akkreditierungsregelungen im BDSG

§ 39 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.

Neues BDSG: Verweis auf AkkStelleG

- § 2 Absatz 3 Satz 2 AkkStelleG: **Die Akkreditierungsstelle lässt Begutachtungen für die in § 1 Absatz 2 Satz 2 genannten Bereiche von den die Befugnis erteilenden Behörden ausführen.**

- § 4 Absatz 3 AkkStelleG: Bei Akkreditierungen für die in § 1 Absatz 2 Satz 2 genannten Bereiche trifft die **Akkreditierungsstelle die Akkreditierungsentscheidung im Einvernehmen mit den Behörden**, die die Begutachtung nach § 2 Absatz 3 durchführen.

Neues BDSG: Verweis auf AkkStelleG

- § 10 Absatz 1 Satz 1 Nummer 3 AkkStelleG: Die Beleihung ist nur zulässig, wenn die zu beleihende juristische Person des Privatrechts einen Akkreditierungsausschuss eingerichtet hat, der im Innenverhältnis in den in § 1 Absatz 2 Satz 2 genannten Bereichen die Akkreditierungsentscheidung trifft. Bei dessen Besetzung ist sicherzustellen, dass **zwei Drittel der Mitglieder aus sach- und fachkundigen Personen, die Angehörige der die Befugnis erteilenden Behörden sind**, berufen werden. Dazu sind den in § 8 Absatz 1 genannten Bundesministerien entsprechende Entsenderechte einzuräumen, die sie unter Einbeziehung der nach § 5 Absatz 8 zuständigen Fachbeiräte ausüben.

Artt. 42 und 43 DSGVO: Grundstruktur

- Wie sind die Akkreditierungskriterien?
  - Werden durch die Aufsichtsbehörde festgelegt
    - Basis: ISO 17065 / Datenschutz-Ausschuss (Nachfolger der Art.-29-Datenschutzgruppe)
    - Stellungnahme Ausschuss (Art. 64 Abs. 1 lit. c DSGVO)
- Wie sind die Zertifizierungskriterien?
  - Werden durch Aufsichtsbehörden oder Datenschutz-Ausschuss (Art. 68 DSGVO) genehmigt
- Einbindung Aufsichtsbehörden in Zertifizierungen?
  - Art. 43 Abs. 1 S. 1 DSGVO: Vor Zertifizierung werden Aufsichtsbehörden unterrichtet

Artt. 42 und 43 DSGVO: Grundstruktur

- Wie ist das Zertifizierungsverfahren?
  - Zertifizierungsstelle legt dieses fest
  - Freiwillig und transparentes Verfahren
  - Einstufig? Zweistufig?

- Wird es ein europäisches Datenschutzsiegel geben?
  - Wenn Kriterien durch den Datenschutzausschuss genehmigt werden, dann kann dieses nach Art. 42 Abs. 5 S. 2 DSGVO zu einer „gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen".

Artt. 42 und 43 DSGVO: Grundstruktur

- Kann sich die Kommission einmischen?
  - Art. 43 Abs. 8 DSGVO: Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zu erlassen, um die **Anforderungen festzulegen**, die für die in Artikel 42 Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind.
  - Art. 43 Abs. 9 DSGVO: Die Kommission kann **Durchführungsrechtsakte** erlassen, mit denen **technische Standards** für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie Mechanismen zur **Förderung und Anerkennung** dieser Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

ULD-Zertifizierung

- Das ULD kann selber ohne Akkreditierung zertifizieren (Art. 42 Abs. 5 DSGVO)
- Beschränkung auf Zuständigkeit / Hoheitsgebiet
- Keine Unterscheidung öffentlicher / privater Bereich
- Wir prüfen selber
  (organisatorische Trennung innerhalb des ULD)

Zeitplan

- Aktuell: Abstimmung Ergänzungen zur ISO 17065 für Akkreditierungen
  - Danach Vorlage beim Datenschutz-Ausschuss zur Stellungnahme
- Abstimmung über Gestaltung von Kriterienkatalogen bzw. Zertifizierungsprogrammen
- November: Informationsveranstaltung für potentielle Zertifizierungsstellen

Weitere Zertifizierungen

- Streitig, ob andere Datenschutz-Zertifizierungen außerhalb der DSGVO noch möglich sind

- Jedoch weitere Zertifizierungen zur Datensicherheit:
  - u.a. ISO 27001 bzw. Zertifizierung auf Basis von IT-Grundschutz

Vielen Dank!

Noch Fragen?

Henry Krasemann
ULD7@datenschutzzentrum.de
Tel. 0431-988 1398

https://www.datenschutzzentrum.de/