Aktiv voran: Neue Möglichkeiten der Zertifizierung für Unternehmen und Verwaltung durch die DSGVO Teil 1

Henry Krasemann

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sommerakademie am 18.09.2017 in Kiel

Warum braucht der Datenschutz ein eigenes Gütesiegel?

- Betroffene: Gefühl, dass ohnehin keine Kontrolle mehr über die (eigenen) Daten besteht
- Vertrauen aufbauen, dass Anbieter rechtskonform handelt und Stand der Technik nutzt
- Unklarheit bei Anwendern / Beschaffern über die Anforderungen im Bereich Datenschutz
  - Stand der Technik?
  - Recht?

Bisher: Audit / Zertifizierung in Schleswig-Holstein

- Auditierung
  - Verfahrensbezogen
  - Datenverarbeitung in einem Unternehmens oder einer Behörde oder einem Teilbereich dieser Organisation
  - Datenschutzorganisation
  - Datenschutzmanagement

- Zertifizierung
  - Produktbezogen
  - „Produkt“ eines Anbieters (Hardware, Software oder IT-Dienstleistung)
  - Ermöglichung oder Erzwingung des datenschutzgerechten Einsatzes beim Anwender durch technische oder organisatorische Vorgaben

Datenschutzaudit nach dem Landesdatenschutzgesetz Schleswig-Holstein

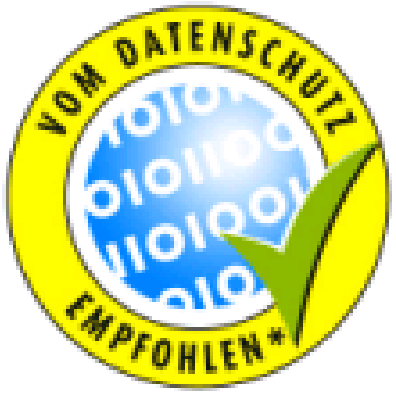
§ 43 Abs. 2 LDSG SH

Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

Einführung des Gütesiegels 2001

§ 4 Abs. 2: Produktaudit (Gütesiegel)

Vorrangiger Einsatz von Produkten, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurden.



Datenschutz-Gütesiegelverordnung

- Zertifizierungsfähige IT-Produkte:
  „Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind“
- Regelung des Zertifizierungsverfahrens:
  - Begutachtung durch externe Sachverständige
  - Inhalt des Gutachtens
  - Kurzgutachten zur Veröffentlichung
- Regelung der Anerkennung von Sachverständigen
- Ermächtigung zur Erhebung von Gebühren

Ablauf des Verfahrens

Produkt
- Eignung für s.-h. Verwaltung
- Herstellungsort beliebig
- Realer Einsatz beliebig

Sachverständige
- Akkreditiert
- Eignung geprüft
- Recht und Technik

Begutachtung
- Zugrundelegung der Kriterien
- Gutachten

Zertifizierung durch das ULD

Überprüfung des Gutachtens
a. Rückfragen
b. Verleihung des Gütesiegels mit Veröffentlichung des Kurzgutachtens

Akkreditierte Sachverständige

- Hohe materielle und formelle Anforderungen (vergleichbar IHK-Gutachtern) bei der Akkreditierung

- Beschränkung der Anerkennung auf die Teilbereiche Recht oder Technik möglich

Neue Aufgaben für alle Aufsichtsbehörden nach DS-GVO

Art. 57 DS-GVO: „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 DS-GVO: 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 ...

Kurz gesagt:

- Datenschutzaufsichtsbehörden **müssen** an der Akkreditierung von Zertifizierungsstellen mitwirken.

- Datenschutzaufsichtsbehörden **dürfen** auch selber zertifizieren.

Art. 42 und 43 DS-GVO: Grundstruktur

- Wer kann zertifizieren?
  - Aufsichtsbehörden und akkreditierte Zertifizierungsstellen (Art. 42 Abs. 5)
- Was wird zertifiziert?
  - Dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird (Art. 42 Abs. 1)
  - Beinhaltet wohl auch Produkte
- Bindung der Aufsichtsbehörden?
  - Nein: Art. 42 Abs. 4

Art. 42 und 43 DS-GVO: Grundstruktur

- Wie wird man (neben den Aufsichtsbehörden) Zertifizierungsstelle? (Voraussetzungen in Art. 43)
  - Akkreditierung durch Aufsichtsbehörde oder nationale Akkreditierungsstelle (in Deutschland: Deutsche Akkreditierungsstelle GmbH (DAkkS))
    - Staat legt fest, ob beide akkreditieren oder nur einer
  - Nachweis von Unabhängigkeit, Fachwissen, keine Interessenskonflikte
  - Genehmigte Kriterien
  - 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

- § 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

- § 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.

Art. 42 und 43 DS-GVO: Grundstruktur

- Wie sind die Akkreditierungskriterien?
  - Werden durch die Aufsichtsbehörden auf Basis ISO 17065 festgelegt
  - Zusammenarbeit der DAkkS
  - AG Zertifizierung entwickelt Vorschlag
  - Art. 29-Gruppe plant Entwurf
- Wie sind die Zertifizierungskriterien?
  - Werden durch Aufsichtsbehörden oder Datenschutzausschuss (Art. 68) genehmigt
  - Überlegung: Muster entwickeln?
    - Modular? Abstrakt? Standard-Datenschutzmodell (SDM)?

Art. 42 und 43 DS-GVO: Grundstruktur

- Wie ist das Zertifizierungsverfahren?
  - Zertifizierungsstelle legt dieses fest
  - Freiwillig und transparentes Verfahren
  - Offen: 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 zu einer „gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen“.
    - Wer ist hier „gemeinsam“?
    - Wann „kann“?

Art. 42 und 43 DS-GVO: Grundstruktur

- Kann sich die Kommission einmischen?
  - Art. 43 Abs. 8: 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: 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.

Vorteile der Zertifizierung

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

Offene Fragen

- Welche Aufsichtsbehörde ist für wen und was zuständig?
  - Zuständigkeit abgestellt auf „Hoheitsgebiet“ und Niederlassung der Zertifizierungsstelle
    - LfDs vs. BfDI
- Zweistufiges Verfahren (Gutachter – Zertifizierungsstelle) weiterhin zulässig?
- Widerrufsverfahren (auch bzgl. „fremder“ Zertifizierungen)?
- Gebühren?
- U.v.m.

Noch Fragen?

https://www.datenschutzzentrum.de/audit/

https://www.datenschutzzentrum.de/guetesiegel/