# Push für Audit und Zertifizierung mit der Datenschutz-Grundverordnung

Henry Krasemann

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sommerakademie am 19.09.2016 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?

# 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.

# Auditverfahren

- Auf freiwilliger Basis (Vertrag mit dem ULD)
- Gegenstand des Audits:
  - Behörden
  - Abgrenzbare Teile von Behörden
  - Einzelne Verfahren
- Voraudit und Hauptaudit
- Durchführung des Auditverfahrens in 3 Schritten
  - Bestandsaufnahme
  - Festlegung der Datenschutzziele
  - Einrichtung eines Datenschutzmanagementsystems
- Begutachtung des Prozesses durch das ULD
- Auditverleihung
  - Veröffentlichung des Kurzgutachtens des ULD
  - Befristung des Audits für 3 Jahre

# Das Datenschutz-Gütesiegel SH des ULD

# *Wichtige Faktoren für Hersteller und Anwender*

## Verbindlichkeit des Zertifikats:

- Zertifizierung durch Datenschutzaufsichtsbehörde
- Problem: bundes- oder europaeinheitliche Lösung
- Transparenz der Prüfergebnisse ermöglicht Nachvollziehbarkeit der Prüfung

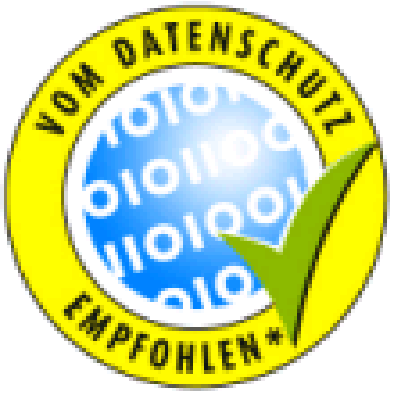
## Vertrauen in das Zertifikat:

- Durch unabhängige, neutrale und kompetente Zertifizierungsstelle
- Durch Transparenz der Prüfergebnisse, ermöglicht Vergleich ähnlicher Produkte

# 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.



# Datenschutzgütesiegelverordnung

- 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

# Einsatzbereiche der zertifizierten Produkte

## Haupteinsatzbereiche:

Targeting-Lösungen
Sicherer Internetanschluss
Archivierungssystem
E-Government-Anwendung
Sozialdatenverarbeitung
Medizinbereich
Datenträgervernichtung
Verwaltungsdokumentation
Sonstiges (Elster, Kollaborationstool, Qualitätssicherung, Bonuskartensystem, Handyparken, Updateservice, WGA, SPP etc.)

# Dauer und Kosten der Gütesiegelverfahren

- Phase 1: Begutachtung durch Sachverständigen
  - Dauer und Kosten abhängig von:
    - Qualität des Produkts
    - Qualität und Vollständigkeit der Dokumentation
  - Kosten frei verhandelbar

- Phase 2: Überprüfung durch das ULD
  - Dauer und Kosten abhängig von:
    - Qualität des Produkts und der Dokumentation
    - Qualität des Gutachtens
  - Kosten nach Gebührensatzung
    - Grundgebühr (in der Regel 1280,- bis 3840,- Euro)
    - Erstattung zusätzlichen Aufwands durch Zusatzgebühren

# *Rezertifizierung*

- Gütesiegel ist auf 2 Jahre befristet
- Regelfall: Rezertifizierung in *vereinfachtem* Verfahren nach Ablauf des Gütesiegels: Lediglich *Änderungen* des Produktes, der Technik- und Rechtslage und der Bewertung werden berücksichtigt.
- Bei umfangreicheren, *erheblichen* Änderungen des Produktes oder der Technik- und Rechtslage: Rezertifizierung auch *während* der Laufzeit
- Bei unerheblichen Veränderungen des Produktes: Anzeige gegenüber dem ULD

# Nutzen und Vorteile eines Datenschutz-Gütesiegels I

Für den Beschaffer / Anwender:

- Sicherheit darüber, ein datenschutzgerechtes Produkt zu nutzen (inkl. Rechtskonformität im Rahmen der Anwendungshinweise)
- Soweit das Produkt die datenschutzgerechte Anwendung durch Technik erzwingt: Keine Datenschutzverletzungen durch Handlungsspielräume der Anwender, Risikoverminderung
- Geprüfte Produktdokumentation in der Regel mit Hinweisen zur datenschutzgerechten Anwendung für Administratoren und Anwender (inkl. Einsatzumgebung)
- Erleichterungen bei der Vorabkontrolle sowie beim Test und der Freigabe neuer Verfahren und Programme
- Transparenz über Vorgänge der Datenverarbeitung
- Erleichterung bei der Beschaffung durch Vergleichbarkeit und Nutzung der Zertifizierungsergebnisse (Kurzgutachten, ggf. ausführliches Gutachten)

# Nutzen und Vorteile eines Datenschutz-Gütesiegels II

Für den Hersteller:

- Wettbewerbsvorteile durch
  - Vorrangiger Einsatz bei Ausschreibungen in Schleswig-Holstein (und ggf. anderen Bundesländern)
  - Einfacherer Nachweis von Datenschutz- und Sicherheitseigenschaften des Produktes gegenüber Kunden
  - Imagegewinn: Nachweis von „Verantwortungsbewusstsein“
- Eigenrevision und „Zwang“ zur Qualitätssicherung und Produktdokumentation (Dokumentation auch von Produktänderungen!)

# Berücksichtigung des Gütesiegels bei Vergabeentscheidungen in SH

- § 4 Abs. 2 LDSG SH: Zertifizierte Produkte sollen vorrangig eingesetzt werden.
- Gütesiegel ist als Kriterium bei der Vergabe zu berücksichtigen.
- Datenschutzgerechte Einsatzmöglichkeit als Leistungsmerkmal des Produkts.
- Wird in der Praxis bei Ausschreibungen berücksichtigt. GMSH als zentrale Beschaffungsstelle z.B. erkennt das Gütesiegel als Vergabekriterium an.
- Führt in Bereichen dazu, dass Wettbewerber sich ebenfalls zertifizieren lassen (z. B. Aktenvernichtung, Meldeauskunft).
- Es wurden auch Vergabeentscheidung gegen zertifizierte Produkte getroffen – andere Kriterien waren Ausschlag gebend. Gütesiegel ist kein alleiniges Qualitätsmerkmal.

# Außerhalb von Schleswig-Holstein

- Weitere Aufsichtsbehörden:
  - Bremen: Audit (aktuell nicht)
  - Mecklenburg-Vorpommern: Gütesiegel („in Benehmen setzen“ – bisher kein Siegel verliehen)
  - Hamburg: Pläne

- Viele private Anbieter
  - Z. B. EuroPriSe GmbH
  - Siehe auch: https://stiftungdatenschutz.org/zertifizierungsubersicht/

# 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 ...

# 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 Auftragsdatenverarbeitern 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 (z. B. ggf. Deutsche Akkreditierungsstelle GmbH?)
    - Staat legt fest, ob beide akkreditieren oder nur einer
      - In Deutschland wohl beide
  - Nachweis von Unabhängigkeit, Fachwissen, keine Interessenskonflikte
  - Genehmigte Kriterien
  - Zertifizierungsverfahren erlassen (inkl. Widerruf etc.)
  - Beschwerdeverfahren

# Art. 42 und 43 DS-GVO: Grundstruktur

- Wie sind die Akkreditierungskriterien?
  - Werden durch die Aufsichtsbehörde festgelegt
  - AG Zertifizierung entwickelt Vorschlag
  - Art. 29-Gruppe plant Entwurf

- Wie sind die Zertifizierungskriterien?
  - Werden durch Aufsichtsbehörden oder Datenschutzausschuss (Art. 68) genehmigt
  - AG Zertifizierung: ggf. 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
  - 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 Auftragsdatenverarbeiters 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“
    - 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/