Datenschutz-Audit und Gütesiegel –
Vorteile für Unternehmen, Erfahrungen und neue Entwicklungen auf europäischer Ebene

Marit Hansen, Henry Krasemann

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Landesdatenschutzkonferenz Rheinland-Pfalz 2015

Mainz, 15.10.2015

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Warum Evaluation und Zertifizierung?
2. Datenschutz-Audit Schleswig-Holstein
3. Datenschutz-Gütesiegel Schleswig-Holstein
4. Entwicklungen auf europäischer Ebene
5. Fazit

1. Warum Evaluation und Zertifizierung?

1. Warum Evaluation und Zertifizierung?

Vertrauen ist gut, Kontrolle sei besser? Aber der muß man auch erst mal vertrauen.

(Erhard Blanck)

gutezitate.com

Warum ein Datenschutz-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?
- Wichtig: Vertrauenswürdigkeit

Gesetzliche Regelungen

§ 9a Bundesdatenschutzgesetz: Datenschutzaudit

in 2001 eingeführt

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.

Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

Vergleichbare Regelungen

- Bundesrecht
  - § 78 c Sozialgesetzbuch X
- Landesrecht
  - § 11 b Abs. 2 Brandenburgisches Datenschutzgesetz
  - § 7 b Bremisches Datenschutzgesetz
  - § 5 Abs. 2 Landesdatenschutzgesetz Mecklenburg-Vorpommern
  - § 4 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen
  - § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein

„Audit“-Terminologie: Auditierung & Zertifizierung

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

Source: kecia85

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

2. 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

3. Das Datenschutz-Gütesiegel SH des ULD

2007: Ministerpräsident übergibt Gütesiegel (Ausnahme)

Wichtig für Hersteller & Anwender

Verbindlichkeit des Zertifikats:

- Zertifizierung durch Datenschutzbehörde
- 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 LDSG SH: Produktaudit (Gütesiegel)

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

Datenschutzgütesiegelverordnung S-H

- 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

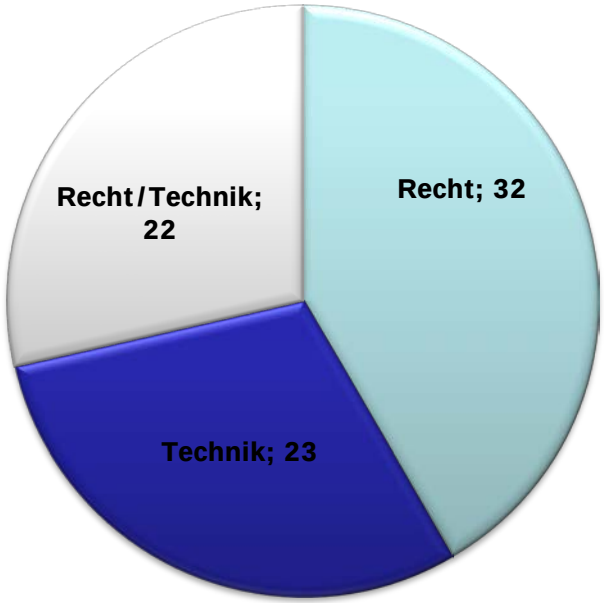
Überprüfung des Gutachtens
a. Rückfragen
b. Verleihung des Gütesiegels mit Veröffentlichung des Kurzgutachtens

Akkreditierte Sachverständige

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

- Beschränkung der Anerkennung auf die Teilbereiche Recht oder Technik möglich

- 76 Sachverständige (Stand 15.10.2015)



Dauer und Kosten der Gütesiegelverfahren

- Phase 1: Begutachtung durch Sachverständige
  - 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

Register der Gütesiegel

Registernr. und Datum	Bezeichnung	Einsatzbereich (Kurzbezeichnung)
03-09/2015 Zertifiziert am 28.09.2015 Befristet bis: 28.09.2017	HealthDataSpace Version 2 Kurzgutachten	Webbasierter, virtueller Datenraum zum Hochladen, Speichern, Verwalten und Austauschen von medizinischen Daten
07-10/2013 Zertifiziert am 13.08.2015 Befristet bis: 13.08.2017 Erstzertifizierung: 17.10.2013	Business Keeper Monitoring System (BKMS) Version 3.1 Kurzgutachten	Dialog zwischen Hinweisgebern und Hinweisbearbeitern, um Missstände, Gefahren und Risiken in einer Organisation melden zu können (Whistleblowing)
01-02/2013 Rezertifiziert am 07.08.2015 Befristet bis 07.08.2017	WIMES (Stand Juni 2015) Kurzgutachten	Web-Portal zur Evaluation der Wirksamkeit von Hilfen zur Erziehung, die von Trägern der öffentlichen Jugendhilfe (Leistungsträger) gesteuert und von freien Trägern der Jugendhilfe und von gewerblichen Dienstleistern (Leistungserbringer) durchgeführt werden.

Rezertifizierung

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

Einsatzbereiche der zertifizierten Produkte

Haupteinsatzbereiche:

- Targeting-Lösungen
- Sicherer Internetanschluss
- Archivierungssysteme
- E-Government-Anwendungen
- Sozialdatenverarbeitung
- Medizinbereich
- Datenträgervernichtung
- Verwaltungsdokumentation
- Sonstiges (Elster, Kollaborationstool, Qualitätssicherung, Bonuskartensystem, Handyparken, Updateservice etc.)

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 benannt.
- Wird in der Praxis bei Ausschreibungen berücksichtigt. GMSH (Gebäudemanagement S-H) 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 ausschlaggebend. Gütesiegel ist kein alleiniges Qualitätsmerkmal.

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)

Vorteile eines Datenschutz-Gütesiegels II

Für den Hersteller:

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

Datenschutz-Gütesiegel auf Bundes- und Länder-Ebene

- In der Regel gesondertes Zertifizierungsverfahren (durch Bundes- oder Landesgesetz) erforderlich, d. h. keine unmittelbare Geltung des ULD-Gütesiegels in anderen Bundesländern.

- Bsp. Mecklenburg-Vorpommern

> § 5 Datenvermeidung, Datenschutzaudit, Systemdatenschutz
> ...
> (2) Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

seit 2015
durch EuroPriSe

- Rolle der Stiftung Datenschutz?

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz

DATENSCHUTZGÜTESIEGEL

HINTERGRUND

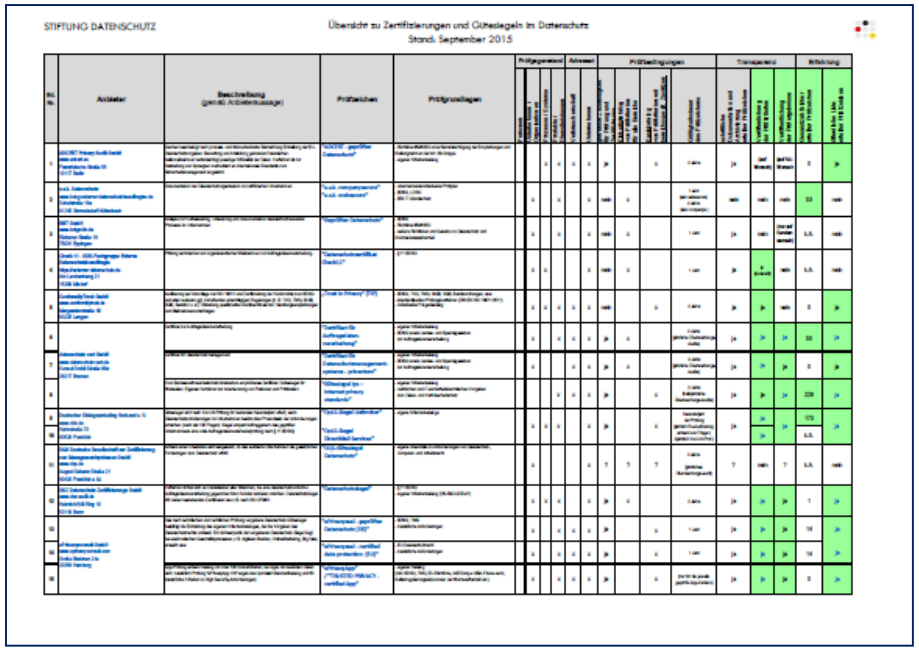
Gütesiegel und Zertifikate zum Datenschutz können als unterscheidende und werbende Merkmale der geprüften und ausgezeichneten Produkte, Dienstleistungen oder Unternehmen eingesetzt werden. Sie erleichtern Kunden die Entscheidung zwischen verschiedenen Anbietern und Angeboten und können zugleich das Vertrauen in neue Technologien fördern. Glaubwürdige Prüfzeichen setzen für Unternehmen Anreize, hohe datenschutzrechtliche Anforderungen einzuhalten oder zu übertreffen: Sie belohnen den dafür betriebenen Aufwand mit einer zusätzlichen Werbemöglichkeit und bestenfalls echten Wettbewerbsvorteilen.

Da die Bundesregierung der Stiftung bislang nicht die Mittel zum Aufbau eines eigenen Zertifizierungssystems gegeben hat, konzentrieren wir uns zunächst auf Herstellung von mehr Transparenz und Vergleichbarkeit bezüglich der diversen existierenden Prüfzeichen.

Stiftung Datenschutz

- Übersicht zu 35 Zertifizierungen und Gütesiegeln im Datenschutz in Deutschland (Stand: September 2015)

- Kriterien
  - Prüfgegenstand:
  - Adressat
  - Prüfbedingungen
  - Transparenz
  - Erfahrung



https://stiftungdatenschutz.org/

4. Entwicklung auf europäischer Ebene

- Initiativen in anderen Ländern

Organisation	Siegel
CNIL (DS-Behörde Frankreich)	Siegel zu „Privacy Governance Procedures“ (seit Ende 2014)
ICO (DS-Behörde UK)	„ICO Privacy Seal“ (ab 2016)
EDÖB (DS-Behörde CH)	Datenschutzzertifizierung für Datenschutzmanagementsysteme, Produkte, Dienstleistungen, Organisationen

- EuroPriSe – European Privacy Seal
- EU-Datenschutz-Grundverordnung

EuroPriSe
European Privacy Seal

- Einführung als Projekt Juni 2007 – Februar 2009
- EU-Förderung 1,3 Mio.
- Projektpartner aus 8 Ländern
- Markteinführung seit März 2009 durch das ULD
- Mehr als 100 zugelassene Experten in 13 Ländern
- Seit 2014 privatisiert als EuroPriSe GmbH der 2B Advice GmbH

Projektpartner:

CNIL.

Agencia de Protección de Datos de la Comunidad de Madrid APDCM

ERNST & YOUNG

LONDON metropolitan university HRSJ Human Rights & Social Justice Research Institute

TÜVIT

ITA INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

BORKING CONSULTANCY

VaF

EuroPriSe European Privacy Seal → Euro PriSe European Privacy Seal

EuroPriSe-Siegelzeichen

Art. 39 EU-DSGVO "Certification" – Entwurf

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. [...]

(Draft COM (2012)0011)

Art. 39 EU-DSGVO "Certification" – Entwurf

1. The Member States and th… …ourage, in particular at European le… …of data protection certification me… …otection seals and marks, allowing … …assess …tection provided by c… …ers and …a protection certifications … …chanisms … …contribute to the proper application of this Regulation, taking account of the specific features of the various sectors an… …ons.
2. […]

(Draft COM (2012)00…

1a. Any controller or processor may request **any supervisory authority** in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation […] ("EP Position First Reading")

1b. The certification shall be **voluntary**, **affordable**, and available via a process that is **transparent** and not unduly burdensome.

1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named **"European Data Protection Seal"**.

nachgewiesene

Fazit: Es geht um Qualität.

5. Fazit

- Gute Erfahrungen des ULD mit dem Gütesiegel
- Künftig in Europa: „European Data Protection Seal“
- Datenschutz ≠ Datensicherheit
- Audits und Gütesiegel:
  - Bewusstsein für eigenen Umgang mit Daten
  - Sichtbarkeit verantwortungsbewussten Handelns
  - Vorteile in Beschaffungsverfahren möglich

Fragen?

www.datenschutzzentrum.de/audit/

www.datenschutzzentrum.de/guetesiegel/