# Tue Gutes und rede darüber – Zertifizierungen für mehr Vertrauen in IT?

Henry Krasemann
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

**Sommerakademie 2015**
31.08.2015

ULD www.datenschutzzentrum.de

## *Was Sie erwartet*

- Normen rund um die IT-Sicherheit (von LDSG bis ISO)
- Typische (Vertrauens-) Probleme der IT
- Datenschutz-Audit Schleswig-Holstein
- Datenschutz-Gütesiegel Schleswig-Holstein
- Ausblick

# Gütesiegel über Gütesiegel




# Regelungen IT-Sicherheit

- § 5 LDSG
  - Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit, Intervenierbarkeit
  - Test und Freigabe
  - Datenschutzverordnung Schleswig-Holstein

- Anlage zu § 9 BDSG
  - Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, getrennte Verarbeitung

# ISMS/DSMS

- IT-Grundschutz-Katalog (BSI) -> normaler Schutzbedarf
  - ISO 27001-Zertifizierung auf Basis IT-Grundschutz
- British Standard 7799
- Ziel: Information Security Management System (ISMS) bzw. Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern
- Notwendig: Datenschutzmanagementsystem (DSMS)

ULD www.datenschutzzentrum.de

# IT-Infrastruktur
# Vertrauensproblem: Struktur

- Auslagerung auf Dritte
  - Problem: Auftragsdatenverarbeitung (ADV) ohne Auftragsdatenverarbeitungsvertrag
  - Problem: Betreiber außerhalb EU in unsicherem Drittland
    - Google, Amazon etc.
      - Selbst bei Zusicherung einer EU-Servernutzung ggf. Zugriff aus USA durch Admins (auf Anordnung Gericht)
- Externe Dienstleister
  - Z. B. Wartung, Datenträgervernichtung etc.
  - ADV ohne ADV-Vertrag ...

# IT-Infrastruktur
# Typische Probleme

- Mandantentrennung
- Verfügbarkeit
  - Problem z. B. bei kostenlosen Diensten
- Verschlüsselte Übermittlung
  - Siehe z. B. neuen § 13 Abs. 7 TMG
- Verschlüsselte Speicherung
  - Problem Datenbankverschlüsselung
- Backup
- Revisionssichere Protokollierung
  - Inkl. rechtzeitige Löschung

ULD www.datenschutzzentrum.de

# Audit und Datenschutz-Gütesiegel Schleswig-Holstein

# 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?



# Gesetzliche Regelungen

§ 9a Bundesdatenschutzgesetz:

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende 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

ULD www.datenschutzzentrum.de

# Audit / Zertifizierung

- 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.

ULD www.datenschutzzentrum.de

## *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


ULD www.datenschutzzentrum.de

# 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 LDSG SH: Produktaudit (Gütesiegel)

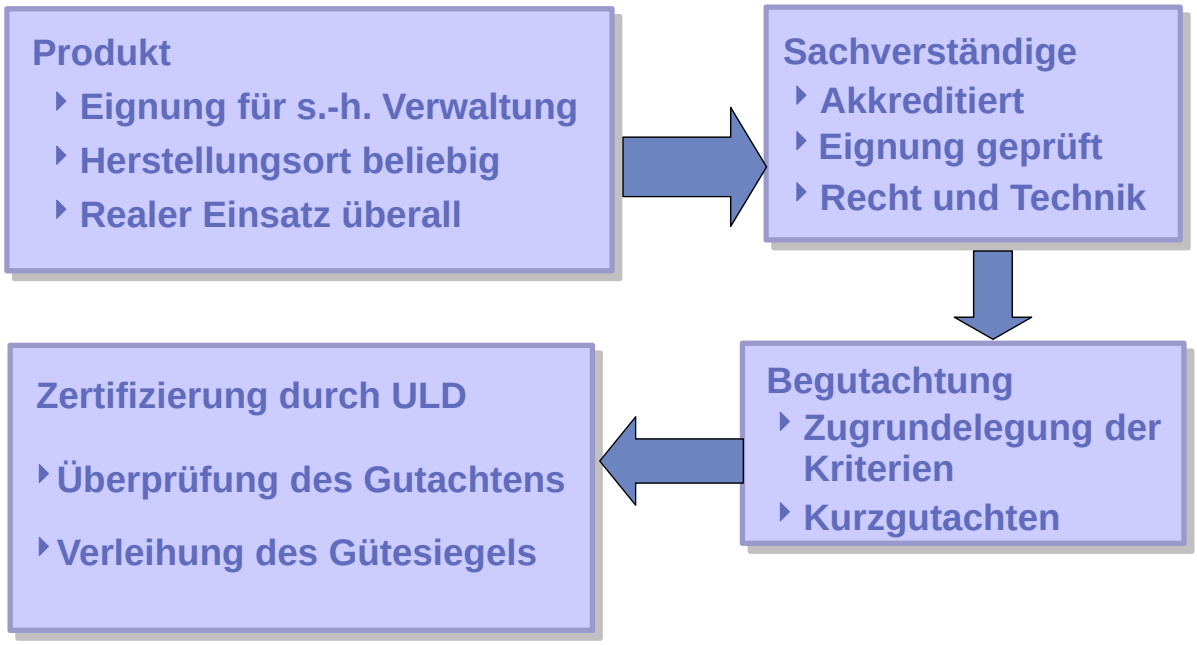
Vorrangiger Einsatz von Produkten, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurden.


ULD www.datenschutzzentrum.de

# 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




www.datenschutzzentrum.de

# 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!)

ULD www.datenschutzzentrum.de

# 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 ausschlaggebend. Gütesiegel ist kein alleiniges Qualitätsmerkmal.

# Geltung in anderen Bundesländern

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

ULD www.datenschutzzentrum.de

# 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

Ernst & Young

London Metropolitan University – 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


ULD www.datenschutzzentrum.de

# Fazit

- Typische Probleme der IT-Sicherheit sind mangelhafte (rechtliche und technische) Einbindung von Dienstleistern und Dritten, unzureichende Protokollierung, Verzicht auf Verschlüsselung, unzureichende Mandantentrennung und das Nichtvorhandensein eines Datenschutzmanagementsystems.

- Audits, Gütesiegel und IT-Grundschutz-Zertifikate sind dazu geeignet, den eigenen Umgang mit Daten zu hinterfragen und verantwortungsbewusstes Handeln auch nach außen hin sichtbar zu machen.

## Ausblick

- Stiftung Datenschutz
  - Vermittler zwischen den Zertifikaten
- Auditierungen in anderen Bundesländern
  - Z. B. Bremen, Mecklenburg-Vorpommern
- EU
  - Datenschutz-Grundverordnung Artikel 39

ULD www.datenschutzzentrum.de

## Noch Fragen?

www.datenschutzzentrum.de/audit/

www.datenschutzzentrum.de/guetesiegel/