

Dataming-Systeme und Big Data: alles böse oder bestehen Möglichkeiten zur Zertifizierung?

Henry Krasemann

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Sommerakademie 2013

26.08.2013

Gütesiegel über Gütesiegel



Big Data

- Große Datenmengen
 - Systematische Auswertung: Statistik, Scoring, Tracking, Profiling
- Beispiele:
 - Werbe-Maßnahmen
 - Marktforschung
 - Fraud-Detection
 - Smart Metering
 - Vorratsdatenspeicherung
 - Soziale Netzwerke

Anwendbarkeit Datenschutzrecht

- „Das sind doch nur Statistiken“?
- Personenbezogene Daten
 - Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person
- Anonymität vs. Pseudonymität
- Fazit: In der Regel liegen zumindest pseudonyme Daten vor und die Datenschutzgesetze sind anwendbar

Rahmenbedingungen

- Gesetz oder Einwilligung
 - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
 - Einwilligung informiert und freiwillig
- Zweckbindung
 - Verwendung nur für Erhebungszweck
- Erforderlichkeit und Datensparsamkeit
 - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
 - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Datensicherheit
 - Technische und organisatorische Maßnahmen
- Kontrolle
 - Interner / externer Datenschutzbeauftragter; Audit

Bestehende Zertifizierungen

- Web-Targeting
 - Einsatz von Cookies / Web-Bugs
 - Erkennung / Berechnung von Zielgruppen
 - Datenschutzvoraussetzungen:
 - Opt-In (vgl. Art. 5 Abs. 3 ePrivacy-Richtlinie)
 - Anonymisierung (IP-Adressen / Browser-Fingerprint)
 - Verhinderung der Zuordnung der Cookie-IDs
 - Cookies mit beschränkter Lebenszeit
 - Online-Transparenz (Information und Aufschlüsselung der Daten) / Auskunftsmöglichkeit
 - Verwendung nur für Werbeeinblendung / nicht für Scoring etc.
 - Zeitnahe Löschung / Widerspruchsmöglichkeit

Bestehende Zertifizierungen

- Fraud-Detection (Missbrauchserkennung)
 - Beispiel Kassensysteme
 - Datenschutzvoraussetzungen:
 - Betriebsvereinbarung als Rechtsgrundlage
 - Pseudonyme Speicherung der Daten
 - Trennung der Rollen
 - Anschlagen nur bei „eindeutigen“ Fällen
 - Wissenschaftlich / statistisch belegt bzw. nachvollziehbare Fälle
 - Mehrstufen-Modell zur Aufdeckung des Pseudonyms
 - Transparenz gegenüber Mitarbeitern
 - Löschung so früh wie möglich
 - Gewährung von Auskunftsrechten
 - Verhinderung generelle Verhaltenskontrolle / Performance-Messung

***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
- 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

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.

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)

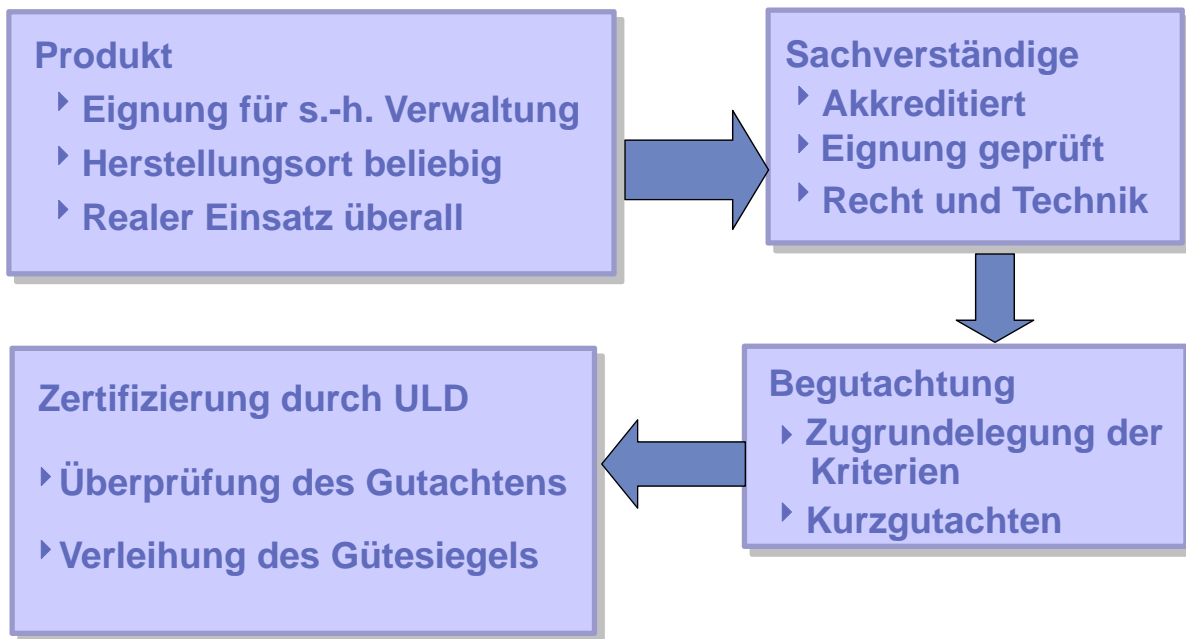
Vorrangiger Einsatz von Produkten, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurden.



Datenschutzauditverordnung 2001

- **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



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 Vergabeentscheidungen gegen zertifizierte Produkte getroffen – andere Kriterien waren Ausschlag gebend. Gütesiegel ist kein allgemeines Qualitätsmerkmal.

Geltung in anderen Bundesländern

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

EuroPriSe European Privacy Seal

- ✓ Einführung als Projekt Juni 07 – Februar 09
- ✓ EU-Förderung 1,3 Mio.
- ✓ Projekt-Partner aus 8 Ländern 
- ✓ Markteinführung seit März 2009 durch das ULD
- ✓ Mehr als 100 zugelassene Experten in 13 Ländern
- ✓ 31 abgeschlossene Verfahren
- ✓ Unterstützt vom EDPS
- ✓ Vorbildlich lt. französischem Senatsbericht (06/09)
- ✓ Neues Logo seit 08/09

Projekt-Partner:



Agencia de Protección de Datos de la Comunidad de Madrid 



BORKING CONSULTANCY



EuroPriSe-Siegelzeichen

© EuroPriSe®



European Privacy Seal

DE-02301 Valid 2010-08

Länderkennzeichen der
Zertifizierungsstelle

Zertifizierungs-
nummer

Gültig bis
Jahr-Monat

Marketing



BANCO
Guipuzcoano **BGNET PLUS**
La Banca por Internet para particulares de Banco Guipuzcoano


European Privacy Seal
e-pacs
Datenschutz-
gütesiegel
EuroPriSe
DE-080003p
Gültig bis
September 2010




European Privacy Seal
ixquick Web-Suche wurde mit dem ersten EUROPÄISCHEN DATENSCHUTZ-GÜTESIEGEL ausgezeichnet
MEHR...



Microsoft



wunderloop
European Privacy Seal

Ausblick

- Stiftung Datenschutz
 - Zertifizierung angedacht
- Bestrebungen / Auditierungen in anderen Bundesländern
 - Z. B. Bremen, Mecklenburg-Vorpommern
- EU
 - Datenschutz-Grundverordnung Artikel 36

Noch Fragen?

www.datenschutzzentrum.de/audit/

www.datenschutzzentrum.de/guetesiegel/

www.european-privacy-seal.eu