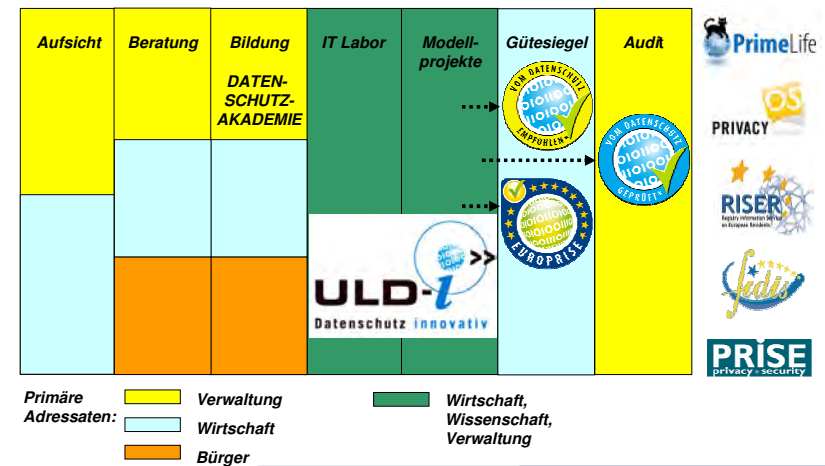


Zertifizierbarkeit von Targeting Techniken

Henry Krasemann
 Unabhängiges Landeszentrum für Datenschutz
 Schleswig-Holstein

eco Arbeitskreis Recht und Regulierung
 03.02.2011

Die 7 Säulen des ULD



Projekte

- Identitätsmanagement – PrimeLife, PRIME und FIDIS
- Europäisches Datenschutz-Gütesiegl - EuroPriSe
- Anonymität im Internet - AN.ON
- Datenschutz in Online-Spielen – DOS
- Audit für Biobanken – bdc-Audit
- Datenschutz in Bürgerportalen
- Europäische Melderegisterauskunft - RISER
- Verbraucherdatenschutz und Datenschutzrecht im Scoring
- Datenschutzerfordernungen für die Forschung – PRISE
- Virtuelles Datenschutzbüro – www.datenschutz.de



Gütesiegel über Gütesiegel



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?
- Datenschutz für beinahe alle Bereiche / Produkte relevant

Gesetzliche Regelungen

§ 9a Bundesdatenschutzgesetz:

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**
 - § 11c Brandenburgisches Datenschutzgesetz
 - § 7b Bremisches Datenschutzgesetz
 - § 5 Abs. 2 Landesdatenschutzgesetz Mecklenburg-Vorpommern
 - § 10a 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.

Das Datenschutz-Gütesiegel des ULD



Einführung des Gütesiegels 2001

§ 4 Abs. 2: Produktaudit (Gütesiegel)

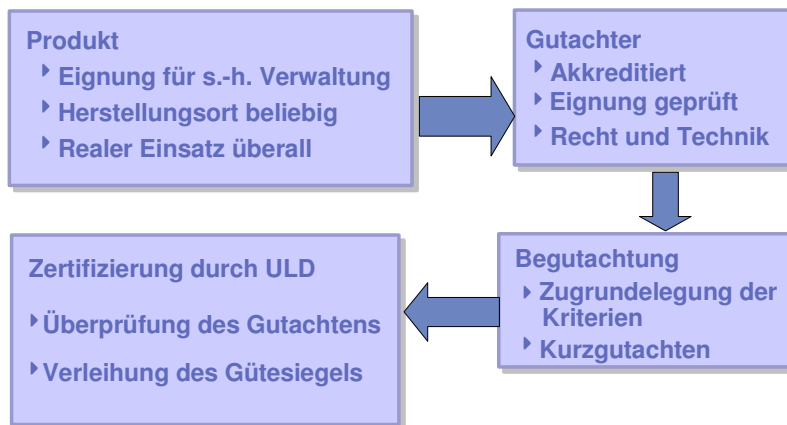
Vorrangiger Einsatz von Produkten, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurden.



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
- Stand November 2010:
 - 44 Einzelsachverständige, davon
 - 20 für den Bereich Recht, 18 Technik, 6 Recht und Technik
 - 9 sachverständige Prüfstellen, davon
 - 1 für den Bereich Recht, 2 Technik, 6 Recht und Technik

Zahl der verliehenen Gütesiegel

2002:	1
2003:	10 (davon 9 gefördert)
2004:	7 (davon 4 gefördert)
2005:	15 (davon 2 Rezertifizierungen)
2006:	10 (davon 5 Rezertifizierungen)
2007:	20 (davon 9 Rezertifizierungen)
2008:	16 (davon 6 Rezertifizierungen)
2009:	12 (davon 6 Rezertifizierungen)
2010:	18 (davon 13 Rezertifizierungen)

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.

EuroPriSe

- Marktvalidierung für ein europäisches Datenschutzgütesiegel
- EU-Förderung: 1,3 Mio
- Laufzeit: Juni 07 – Februar 09
- Konsortium: 9 Partner aus 8 Ländern
- Unterstützt vom EDPS
- Vorbildlich lt. französischem Senatsbericht (06/09)



European Commission
Information Security and Media



Agencia de Protección de Datos
de la Comunidad de Madrid



BORKING
CONSULTANCY

Fortführung

- Seit März 2009 durch das ULD
- 15+1 erfolgreiche Zertifizierungen (10/2010)
- Antragsteller aus Europa, Nord- und Südamerika
- Über 25 laufende Verfahren
- Über 110 zugelassene Gutachter aus 13 Ländern (58 rechtlich, 52 technisch in 11 EU-Ländern + USA, Argentinien; Stand 12/2010)
- Juvin Report des Europäischen Parlaments zum Einfluss der Werbung auf das Verbraucherverhalten (15.12.2010)

EuroPriSe-Siegel



Das **europäische Datenschutz-Gütesiegel** bestätigt, dass ein IT-Produkt oder eine IT-basierte Dienstleistung in **Vereinbarkeit mit europäischem Datenschutzrecht** eingesetzt werden kann.

Marketing



Stiftung Datenschutz

- Koalitionsvertrag / Eckpunktepapier FDP
- Vorbild: „Stiftung Warentest“
- 1. Säule: Vergabe von Audits (Datenschutzkonzepte) und Gütesiegeln (Produkte / Verfahren)
- Prüfung durch akkreditierte Sachverständige
- Antragsteller: private und öffentliche Stellen
- Online- und Offlineprodukte
- „Mehr“ als nur gesetzliche Vorschriften („Gold“, „Platin“?)
- Freiwillig
- Auf 2 Jahre befristet
- Keine bindende Wirkung gegenüber Aufsichtsbehörden

Stiftung Datenschutz

- 2. Säule: Vergleichende Tests von Produkten und Verfahren
- 3. Säule: Bereitstellen von Bildungsangeboten im Bereich Datenschutz
- 4. Säule: Forschung und Weiterentwicklung des Datenschutzrechts
- Bundesinnenminister Thomas de Maizière (CDU) will die *"Gesamtstrategie Datenschutz"* im Herbst 2010 vorlegen

Targeting

Zertifizierte Targeting Lösungen

- Predictive Targeting Networking (PTN) von Nugg.ad
- Wunderloop Integrated Targeting Platform
- targ.ad von GroupM
- TGPopen von 1&1

Rechtliche Probleme

- IP-Adressen sind personenbeziehbare Daten
- IDs in Cookies sind i. d. R. personenbeziehbare Daten
- § 15 Abs. 3 TMG:
 - Profile nur unter Pseudonym speichern
 - Pseudonyme nicht mit Identifikationsdaten zusammen bringen
 - Widerspruchsrecht und Hinweis auf Widerspruchsmöglichkeit
- Wer ist verantwortliche Stelle?
 - Eigene Datenverarbeitung oder Auftragsdatenverarbeitung?
- Anbieter außerhalb der EU

Lösungen Grundkonstrukt

- Besucher einer Webseite denkt, dass Betreiber der Seite Daten verarbeitende Stelle ist
- IP-Adresse wird an Targeting-Unternehmen „weitergeleitet“
 - = Übermittlung? (Abruf durch Dritte)
- Einwilligungslösung
 - Kaum realisierbar, das Targeting schon vor der Einwilligung gewollt ist
- Auftragsdatenverarbeitung
 - Seitenbetreiber muss Auftragsdatenverarbeitungsvertrag schließen
 - (P) Keine Vermengung von Daten verschiedener Auftraggeber

Lösung IP-Adressen

- Anonymisierungsdienst nutzen
 - Unabhängiger Proxy-Betreiber
 - Keine Speicherung / Protokollierung von IP-Adressen
- Seitenbetreiber beauftragen Anonymisierungsdienst
 - Auftragsdatenverarbeitung

Lösung Cookies

- IDs dürfen nicht mit Identifizierungsdaten zusammengeführt werden
- Lebenszeit des Cookies maximal 6 Monate
- Bei sich erneuernden Cookies:
 - Lebenszeit nur wenige Tage

Lösung Widerspruchsrecht

- Einrichtung z. B. „Widerspruchscookie“
- Seitenbetreiber muss auf Widerspruchsmöglichkeit hinweisen

Neue Telekommunikationsrichtlinie Art. 5 Abs. 3

- Opt-In für Cookies (nicht Session-Cookies)
 - Informierte Einwilligung des Nutzers erforderlich
 - Einwilligung sollte nur für begrenzten Zeitraum gelten
 - Jederzeit widerrufbar
- Umsetzung in Deutschland steht aus
 - Bis Mai 2011
- Lösungsideen
 - Einwilligung auch durch Browser-Einstellungen?
 - idR nicht ausreichend aktuell
 - Piktogramm auf Webseiten

Weitere Problembereiche

- Wahl der Kategorien
 - Vermeidung Verarbeitung sensibler Daten
 - Andernfalls Einwilligung erforderlich
 - Problematisch z. B.: „homosexuell“, „schwanger“
 - Keine Kategorien, die sich an Kinder richten
- Geolokalisierung
 - Düsseldorfer Kreis
 - IP-Adresse vor Geolokalisierung um 1-2 Oktette kürzen

Weitere Problembereiche

- Profile sollten nur eine beschränkte Lebenszeit haben
- Gewährleistung von Auskunfts-, Berichtigungs-, Lösungs- und Widerspruchsrechten
 - Vollständige Auskunft
 - Z.B. Abruf der Kategorien

Noch Fragen?

www.datenschutzzentrum.de/guetesiegel/

www.european-privacy-seal.eu