Zertifizierungen im Datenschutz - Chancen international und Nutzen?

Sebastian Meissner
Head of the EuroPriSe Certification Authority

3. Hamburger Datenschutztage
Hamburg, 19.03.-20.03.2015

Grundsätzliches zum Thema Datenschutzzertifizierung

- Ziele
  - Förderung datenschutzfreundlicher Verfahren und Produkte
  - Orientierungshilfe für Unternehmen, Behörden und Verbraucher
  - (Teilweise) Kompensation des bestehenden Vollzugsdefizits
    → Erhöhung des Datenschutzniveaus insgesamt
    („mehr Datenschutz in der Fläche“)
- Vorteile
  - Nachweis von Compliance mit geltendem Datenschutzrecht (B2B und B2C)
  - Wettbewerbsvorteil gegenüber Konkurrenten
  - Erhöhung der Akzeptanz innovativer Produkte und Verfahren
  - Generell: Imagegewinn für die zertifizierte Organisation

Grundsätzliches zum Thema Datenschutzzertifizierung

- Inhalt einer Zertifizierung
  - Minimum: Compliance mit geltendem Datenschutzrecht
  - „Compliance +“: „Übergewährleistung“ des Datenschutzes (z. B. durch ein besonderes Maß an Datensparsamkeit, Transparenz oder Intervenierbarkeit)
- Gesetzliche Regelungen
  - Programmnorm des § 9a BDSG (seit 2001): Datenschutzaudit in Aussicht gestellt, Ausführungsgesetz fehlt bis heute
  - Landesgesetzliche Regelungen: Datenschutzgütesiegel-VO Schleswig-Holstein, Bremische Datenschutzaudit-VO etc.
  - Richtlinie 95/46/EG: Keine Regelungen
  - Datenschutzgrundverordnung: Verschiedene Ansätze

Produkt- vs. Verfahrenszertifizierung

- Produktzertifizierung
  - Hardware / Software
  - Überprüfung einer bestimmten Version des Produkts
  - Produkt macht es der es einsetzenden Stelle leicht, alle Vorgaben des geltenden Datenschutzrechts einzuhalten
  - Hersteller oder Anbieter des Produkts
- Verfahrenszertifizierung
  - Gesamte DV / mehrere Verfahren / ein Verfahren (z. B. konkrete Implementierung eines Personaldatenverarbeitungssystems)
  - Klare Abgrenzung des Zertifizierungsgegenstands erforderlich
  - Compliance des Verfahrens mit geltendem Datenschutzrecht
  - Verantwortliche Stelle / Auftragsdatenverarbeiter

Datenschutzgütesiegel und -zertifikate

- Verschiedene Ansätze
  - Datenschutzaufsichtsbehörde vs. private Zertifizierungsstelle
  - Einstufiges vs. qualitätsgesichertes Verfahren
  - Zertifizierung von nationalem Recht vs. EU-Recht
  - Unterschiede bzgl. Transparenz, Prüfbarkeit & Glaubwürdigkeit
- Sprunghafter Anstieg an Siegeln/Zertifikaten während der letzten Jahre

Eine Siegel- und Zertifizierungsübersicht für Deutschland findet sich unter https://stiftungdatenschutz.org/zertifizierungsubersicht/

Anforderungen an eine vertrauenswürdige Zertifizierung

- Düsseldorfer Kreis
  - Beschluss vom Februar 2014: Benennung von Strukturelementen für eine vertrauenswürdige Zertifizierung

- Vereinfachte Formel

  Transparenz
  \+ Prüfbarkeit
  \+ Glaubwürdigkeit

  = Vertrauen

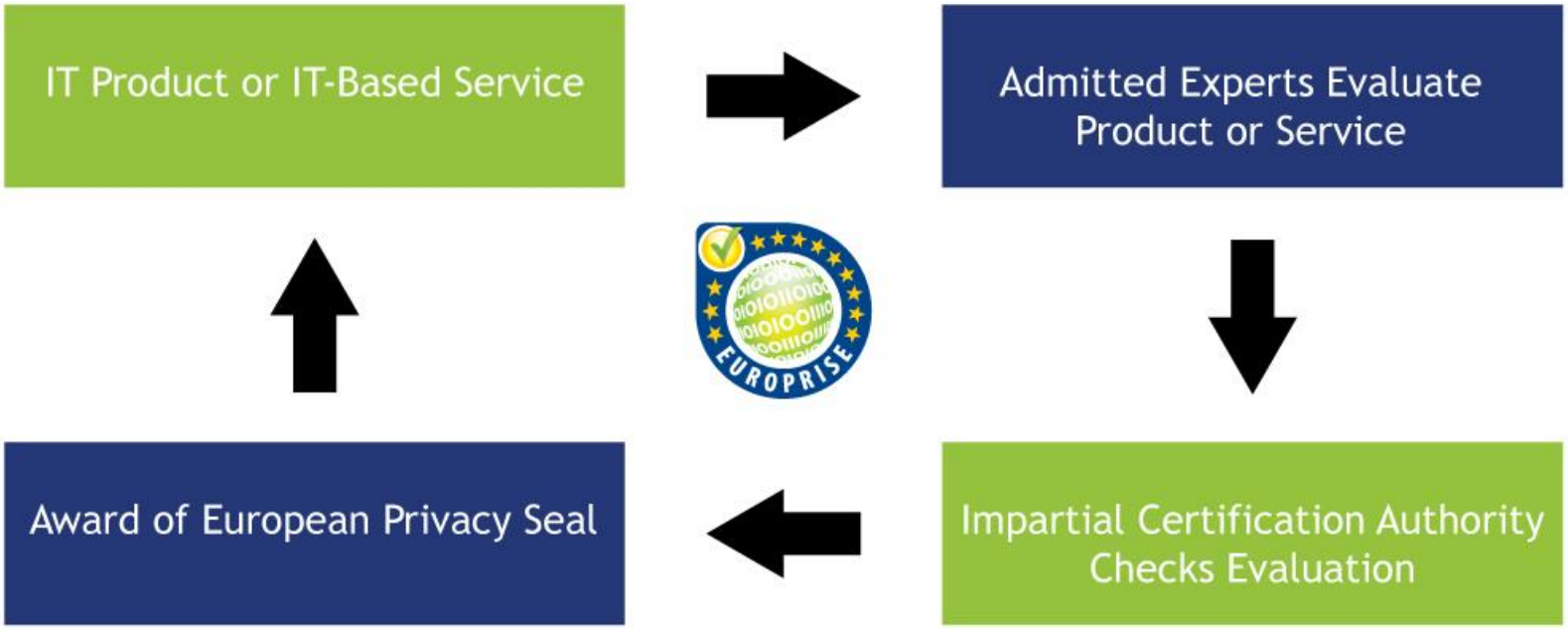
→ Verdeutlichung anhand des European Privacy Seal

EuroPriSe: Zertifizierung von Compliance mit EU-Datenschutzrecht

- EuroPriSe v0.1
  - EuroPriSe-Projekt, gefördert von EU-Kommission
  - Zeitrahmen: 07/2007 – 02/2009
- EuroPriSe v1.0
  - Regelbetrieb 1: ULD, Kiel
  - Zeitrahmen: 03/2009 – 12/2013
- EuroPriSe v2.0
  - Regelbetrieb 2: EuroPriSe GmbH, Bonn
  - Zeitrahmen: Seit 01/2014

Transparenz

des Zertifizierungsverfahrens:



Transparenz

der Zertifizierungskriterien

1. Grundsätzliches
2. Rechtmäßigkeit
3. TOM
4. Betroffenenrechte

Transparenz

der Zertifizierungskriterien

Set 1: Overview on Fundamental Issues

The first set covers **fundamental issues**. Questions posed in this set aim to provide an overall picture of privacy relevant issues relating to the ToE. The first part of the set concerns fundamental processing aspects such as processing operations, processed data, and pursued purposes, while the second part deals with the fundamental technical construction of a product or service, i.e. with topics such as data avoidance/minimisation and transparency.

1.1 Fundamental Aspects of Processing

1.1.1 Processing Operations; Purpose(s)

(Articles 2(b) and 6(1) (b) of Directive 95/46/EC)

Relevant Questions:

- What different processing operations are associated with the use of the product or service?
- What is the main operation?
- What further purposes are or can be served by the product or service?
- Are all the purposes sufficiently specifically defined?
- To which recipients are data disclosed (in-house and externally)? For what purposes?

1.1.2 Processed Personal Data

(Articles 2(a) and 8 of Directive 95/46/EC)

Transparenz → Prüfbarkeit

durch Veröffentlichung der Prüfungsergebnisse (im Erfolgsfall)

European Privacy Seal for Carglass

Carglass GmbH proved that its IT-based service "Interfaces To Insurance Companies" complies with EU data protection law. Customers of Carglass (i.e., vehicle owners) can be sure that processing of their personal data by Carglass when communicating with vehicle insurance companies on the occasion of an insurance event relating to the breakage of glass is in line with the high requirements of EU data protection law.

Product/ Version	Interfaces To Insurance Companies Function as provided in November 2014 **Qualification: IT-based service** View the Carglass Interfaces to Insurance Companies Certificate
Cert. No.	EP-S-8V636C
Validity	13/01/2015 - 31/01/2017
Public Report	Interfaces To Insurance Companies Short Public Report
Manufacturer/ Provider	CARGLASS® Carglass GmbH Godorfer Hauptstr. 175 50997 Köln Germany
BEST	Employees of insurance companies who use the web portal **www.carglass4partners.de** are informed about relevant data protection requirements concerning the transfer of personal data on vehicle owners to Carglass by means of a detailed and comprehensible data protection leaflet. The leaflet is available at **www.carglass4partners.de/datenschutz/merkblatt.html**.
ATTENTION:	n.a.
Summary	The focus of the services that are provided by Carglass GmbH is on the repair or replacement of car windows. Providing the services, Carglass aims at assisting its customers in the overall process which involves communication with vehicle insurance companies. The main purpose of this communication is to clarify whether in a given case the relevant vehicle insurance company will accept the cost of repair.

Glaubwürdigkeit

- Gutachter
  - Fachkunde, Zuverlässigkeit und Unabhängigkeit müssen gewährleistet sein
- Zertifizierungsstelle
  - Fachkunde, Zuverlässigkeit und Unabhängigkeit müssen gewährleistet sein
  - Sicherstellung eines einheitlichen Qualitätsniveaus über verschiedene Zertifizierungsverfahren hinweg (Anwendung der Kriterien, Prüftiefe etc.)
- Instrumente zur Erhöhung der Glaubwürdigkeit
  - Beispiel: EuroPriSe Advisory Board

EuroPriSe Advisory Board

Das Board berät die EuroPriSe-Zertifizierungsstelle, insbesondere zu den folgenden Themen:

- Änderungen an den Prüfkatalogen (insbesondere am EuroPriSe-Kriterienkatalog)
- Einführung neuer Zertifizierungsprodukte (z. B. Websitezertifizierung oder ADV-Zertifizierung)
- Meinungsverschiedenheiten zwischen EuroPriSe-Zertifizierungsstelle und Gutachtern zu technischen oder rechtlichen Grundsatzfragen
- Fragestellungen, die dem Advisory Board durch den gewählten Vertreter der Gutachter präsentiert werden

EuroPriSe Advisory Board

Mitglieder:

Dr. John Borking
Dr. Gwendal Le Grand
Dr. Waltraut Kotschy
Dr. Reinhard Priebe
Peter Schaar
Dr. Thilo Weichert

Beobachterstatus:
Gemma Farmer (ICO)

Foto: EuroPriSe GmbH

Datenschutzzertifizierung international

- Globale Ansätze für eine Datenschutzzertifizierung
  - Gegenwärtig wegen großer Unterschiede bei den gesetzlichen Vorgaben wenig erfolgversprechend
- Datenschutzzertifizierung auf EU-Ebene
  - Status quo: Möglichkeit einer Zertifizierung auf Grundlage der EU-Datenschutzrichtlinien (aber: Compliance mit EU-Recht bedeutet nicht notwendiger Weise auch Einhaltung aller nationalen Regelungen zum Datenschutz)
  - Ausblick: Datenschutzgrundverordnung
    (Vorteile: EU-weit gültige gesetzliche Regelungen zum Thema Datenschutzzertifizierung + generell gesetzliche Regelungen zum Datenschutz, die unmittelbar in allen EU-Mitgliedstaaten gelten)

- Entwurf der EU-Kommission

Artikel 39 DSGVO-E

„Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und –zeichen.“

Inhaltliche Eckpfeiler müssten erst noch durch die EU-Kommission mittels delegierter Rechtsakte und technischer Standards festgelegt werden.

Der Kommissionsentwurf sieht auch keine gesetzlichen Anreize für die Durchführung von Zertifizierungsverfahren vor.

- Vom EU-Parlament beschlossene Fassung von Art. 39
  - Einführung eines Europäischen Datenschutzgütesiegels
  - Zertifizierung durch Datenschutzaufsichtsbehörden (Antrag kann bei jeder Aufsichtsbehörde gestellt werden)
  - Aufsichtsbehörde kann während des Verfahrens spezialisierte dritte Prüfer akkreditieren, die die Prüfung für sie durchführen
  - Zusammenarbeit der Aufsichtsbehörden, um ein harmonisiertes, datenschutzspezifisches Zertifizierungsverfahren zu gewährleisten
  - „Zertifizierung ist freiwillig, erschwinglich & über ein transparentes und nicht übermäßig aufwändiges Verfahren zugänglich“

Beispiele für von Aufsichtsbehörden selbst verliehene Siegel:
ULD-Gütesiegel und „LABEL CNIL“ (Frankreich)

- Gesetzliche Anreize für eine Zertifizierung im Entwurf des EU-Parlaments
  - Garantien bzgl. TOM beim Auftragsdatenverarbeiter: Hinreichende Garantien können durch Zertifizierungsverfahren nachgewiesen werden (Art. 26 Abs. 3a))
  - Siegel kann Übermittlung personenbezogener Daten in einen unsicheren Drittstaat legitimieren (Art. 42 Abs. 2a)aa))
  - Siegel → Haftungserleichterung (Art. 79 Abs. 2b)): Geldbuße für Datenschutzverstoß nur bei Vorsatz oder Fahrlässigkeit

Weiterer möglicher gesetzlicher Anreiz:
Vorrangiger Einsatz zertifizierter Produkte durch öffentliche Stellen (vgl. § 4 Abs. 2 LDSG SH bzw. § 5 Abs. 2 LDSG MV)

- Bisheriger Kompromiss im Rat der EU
  - Zentraler Unterschied zu der vom Parlament beschlossenen Fassung: Zertifizierung auch durch private Zertifizierungsstellen
  - Gemäß Artikel 39a Abs. 1 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt.
  - Die Zertifizierungsstelle wird entweder von der nationalen Aufsichtsbehörde oder der Akkreditierungsstelle akkreditiert.
  - Weitere gesetzliche Anreize vorgesehen (z. B. Erleichterung des Nachweises angemessener TOM durch Zertifizierung)

Beispiel für ein Siegel, das durch private Zertifizierungsstellen nach Akkreditierung durch nationale Akkreditierungsstelle verliehen wird: Künftiges „ICO Privacy Seal“ (Großbritannien – ab 2016)

Datenschutzzertifizierung auf EU-Ebene

- Fazit
  - Einheitliche Datenschutzregelungen auf EU-Ebene und explizite gesetzliche Vorgaben zu Datenschutzzertifizierungen (inklusive gesetzlicher Anreize) bieten eine große Chance für die weitere Entwicklung von Datenschutzzertifizierungen in der EU.
  - Gesichert erscheint, dass die Datenschutzgrundverordnung Regelungen zum Thema Zertifizierung enthalten wird. Die genaue Ausgestaltung dieser Regelungen ist noch ungewiss.
  - Der Nutzen einer Zertifizierung kann durch EU-weit einheitliche Datenschutzregelungen (ein Siegel bedeutet dann Compliance mit Datenschutzrecht in allen Mitgliedstaaten) & klare gesetzliche Anreize beträchtlich erhöht werden.

Vielen Dank für Ihre Aufmerksamkeit !!!

Sebastian Meissner
Head of Certification Authority

Tel.: +49 228 763 679 31
E-Mail: meissner@
european-privacy-seal.eu