



eCompliance

by TÜV®

## **Vertrauenswürdige IuK-Infrastrukturen Nachweis der Konformität durch Zertifizierung**

Fall: E-Postbrief

Monika Wojtowicz, LL.M.  
Dr. Christoph Sutter



# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung
  - Aktuelle Entwicklungen*
- Was ist ein Zertifikat?
- Was soll eine DS-Zertifizierung leisten?
  - Motivation und Erwartungen*
- Verwendbarkeit der Zertifikate
  - Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgemäße Prüfung
  - Beispiel: TÜViT Trusted Site Privacy Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Inhaltsübersicht

- Einführung
- **Datenschutz-Zertifizierung**  
*Aktuelle Entwicklungen*
- Was soll eine DS-Zertifizierung leisten?
- Was ist ein Zertifikat?
- **Verwendbarkeit der Zertifikate**  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- **Zweckgerechte Prüfung**  
*Beispiel: TÜVIT TSP- Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Datenschutz-Zertifizierung

## aktuelle Entwicklung

- Deutschland
  - Stiftung Datenschutz
  - Selbstregulierungsinitiativen der Wirtschaft
  - Zertifizierungsverfahren der Privatwirtschaft
  - Gütesiegel in Schleswig-Holstein und Bremen
  - § 18 III Nr. 4 De-Mail-Gesetz: Datenschutz-Nachweis für die Akkreditierung von De-Mail-Anbietern
  - TÜViT Trusted Site Privacy – quid! Qualität im betrieblichen Datenschutz
- Europa
  - Madrider EntschlieÙung zu internationalen Standards im Datenschutz
  - Art. 29-Gruppe: Stellungnahme zum Grundsatz der Rechenschaftspflicht
  - EU-Kommission: Gesamtkonzept für den Datenschutz in der EU
  - European Privacy Seal (EuroPriSe)

# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung  
*Aktuelle Entwicklungen*
- Was soll eine DS-Zertifizierung leisten?  
*Motivation und Erwartungen*
- Was ist ein Zertifikat?
- Verwendbarkeit der Zertifikate  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgerechte Prüfung  
*Beispiel: TÜVIT TSP- Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Datenschutz-Zertifizierung

## Erwartungen und Motivation

- Instrument der Vertrauensbildung im Verhältnis Bürger, Unternehmen, Staat  
Entschließung des Bundestages zum 22. TB des BfDI
- Stärkung der Eigenverantwortlichkeit der verantwortlichen Stellen  
KOM(2010) 609, WP173 Art. 29-Gruppe
- Wettbewerbsvorteil  
BT-Drs. 14/4329
- Erleichterungen und Entlastungen im Rahmen des § 11 BDSG  
Stellungnahme der BITKOM zum Entwurf des Datenschutzauditgesetzes
- Rechtsverbindlichkeit, Nachweisbarkeit des Geschäftsverkehrs im Internet

# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung  
*Aktuelle Entwicklungen*
- Was soll eine Zertifizierung leisten?  
*Motivation und Erwartungen*
- Was ist ein Zertifikat?
- Verwendbarkeit der Zertifikate  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgerechte Prüfung  
*Beispiel: TÜVIT TSP- Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# DS-Zertifikat

## Begriffsbestimmung

### Zertifikat

- die Feststellung eines **fachkundigen, unparteiischen Dritten**, dass ein Prüfgegenstand bestimmte von einer **unabhängigen Stelle** festgelegte Forderungen (**Regelwerk**) erfüllt.

Regelwerk

Prüfstelle

Zertifizierungsstelle

# DS-Zertifikat

## Der Ball ist rund und ein TÜViT-Zertifikat ist eckig

### Zertifizierungsstelle

(Verband)

#### Eigenschaften

- **unabhängige Stelle**
- **überwacht die Regeln**  
(Nachvollziehbarkeit, Vergleichbarkeit, Wiederholbarkeit, Belastbarkeit)

### Prüfstelle

(Schiedsrichter)

- **unabhängig und akkreditiert**
- **ausgewiesene Fachkenntnis**
- **Objektivität – Neutralität – Erfahrung**

### Regelwerk

(Spielregeln)

- **durch Gesetz / Verordnung vorgegeben**
- **bekannt und anerkannt**
- **einheitlich und transparent**
- **bestimmt die Prüftiefe**

# DS-Zertifizierung

## Relevante Inhalte

### Zertifizierung

- die Bestätigung von **Eigenschaften** eines **Prüfgegenstandes** auf Basis eines vorliegenden **Regelwerkes**



### Was kann bescheinigt werden?

- Nur das was mit dem Regelwerk abgefragt wird !



### Was kann geprüft werden?

- Verfahren
- Produkt
- Organisation

# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung  
*Aktuelle Entwicklungen*
- Was soll eine DS-Zertifizierung leisten?
- Was ist ein Zertifikat?
- **Verwendbarkeit der Zertifikate**  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgerechte Prüfung  
*Beispiel: TÜVIT TSP- Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Was sagt ein Datenschutz-Zertifikat aus?

## Übersicht

Prüfgegenstand	Prüfansatz	Zertifikatsaussage (Kern)
<ul style="list-style-type: none"><li>▪ Produkt</li></ul>	<ul style="list-style-type: none"><li>▪ Materiell-rechtliche Zulässigkeit</li><li>▪ Technische Sicherheit</li><li>▪ Organisatorische Sicherheit</li></ul>	<b>Datenschutzgerechter Einsatz ist möglich</b>
<ul style="list-style-type: none"><li>▪ System</li><li>▪ Verfahren</li><li>▪ Prozess</li></ul>		<b>Datenschutzkonformer Betrieb ist nachgewiesen</b>
<ul style="list-style-type: none"><li>▪ Management-system</li></ul>	<ul style="list-style-type: none"><li>▪ Prüfung des PDCA -Zyklus (Plan - Do - Check - Act)</li><li>▪ Datenschutzgerechte Ausgestaltung der Organisation</li><li>▪ Erfüllung der materiellen Zulässigkeitsvoraussetzungen wird nicht bzw. nur sehr eingeschränkt betrachtet</li></ul>	<b>Organisation ist befähigt, das erreichte Datenschutzniveau dauerhaft aufrechtzuerhalten</b>

# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung  
*Aktuelle Entwicklungen*
- Was ist ein Zertifikat?
- Was soll eine DS-Zertifizierung leisten?
- Verwendbarkeit der Zertifikate  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgerechte Prüfung  
Beispiel: *TÜViT TSP-Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Kann ein Zertifikat diese Erwartungen erfüllen?

## Prüfansatz für den E-Postbrief

- **Prüfgegenstand:**

Eine bereits implementierte Plattform zur rechtsverbindlichen Internetkommunikation

- **Zielsetzung:**

Nachweis der Vertrauenswürdigkeit des Dienstes durch ein Zertifikat

- **Welcher Prüfansatz kann das leisten?**

Nur eine umfassende Verfahrensprüfung

(Analoger Ansatz, wie für den Datenschutz-Nachweis der De-Mail-Dienste-Anbieter nach § 18 III Nr. 4 De-Mail-Gesetz – siehe De-Mail-Kriterienkatalog des BfDI)

# TÜViT Trusted Site Privacy Regelwerk

## ➤ **quid! Qualität im Datenschutz**

*Qualitätsmodell gemeinsam entwickelt von Vertretern des BfDI, der LfDI, des BMAS, von Hochschulen, Wirtschaftsverbänden, Gewerkschaften, Datenschutzinstanzen, Unternehmen und Behörden.*

## Fragenkataloge

### ■ **Funktionsbedingungen bDSB**

Qualifikation – MA-Schulung und -Information – Organisation – QS-Management

### ■ **Betriebe**

Rechtskonformität – Kundenfreundlichkeit – Transparenz – Datensicherheit

### ■ **Arbeitsplätze**

Mitarbeiterfreundlichkeit – Sachkompetenz – DS-Qualitätsmanagement

### ■ **Prozesse**

Rechtskonformität – Betroffenenfreundlichkeit – Transparenz – QS-Management

### ■ **Produkte**

Rechtskonformität – Betroffenenfreundlichkeit – QS-Management

# TSP Privacy Zertifizierung

## Kriterienkatalog Verfahren (quid! Prozesse)

- ✓ **Rechtskonformität**
  - Rechtsgrundlagen, Zweckbindung, Datensparsamkeit, Verpflichtungserklärung..
- ✓ **Kundenfreundlichkeit**
  - Datenschutz-Hinweise, Möglichkeit zum Selbstdatenschutz
- ✓ **Betroffenenfreundlichkeit (Mitarbeiter, Anwender)**
  - Datenschutz-Hinweise, Partizipation, Möglichkeiten zum Selbst-datenschutz , Akzeptanz der technischen und organisatorischen Maßnahmen
  - Information des Anwenders über die eingesetzten IT-Produkten (z. B. Handbücher)
- ✓ **Transparenz**
  - (teil-) öffentliche Datenschutz-Policy , Transparenz der technischen und organisatorischen Maßnahmen
- ✓ **Datenschutz-Qualitätsmanagement**
  - Anpassung des Konzeptes bei Veränderungen (Recht und/oder Technik)
- ✓ **Datensicherheit**
  - Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle, Verschlüsselung, Trennungsgebot
- ✓ **Sicherheitstechnische Untersuchung (SU)**
  - Sicherheit der verwendeten Komponenten, System-Management, Tests und Inspektionen

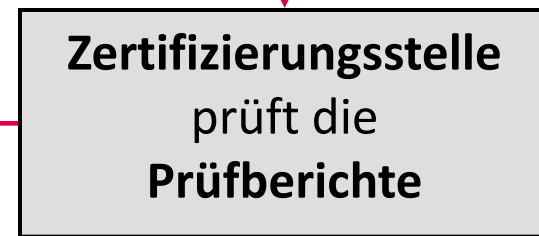
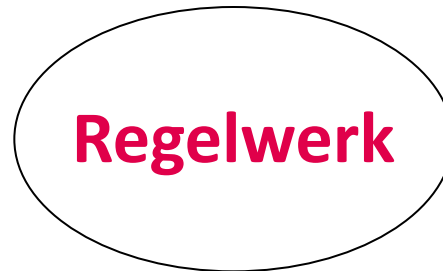
# TSP Privacy Zertifizierung

## Der Zertifizierungsablauf

Prüfgegenstand (Kunde)



Prüfstelle



Zertifizierungsstelle

# TSP Privacy Zertifizierung

## Die Ergebnisdokumente

- **Beschreibung des ToA** – Version 1.0
- **vorläufiges Gutachten Recht** – TÜViT-intern
  - mit zusätzlichen ToA-abhängigen Aufgaben für die SU
- **vorläufiges Gutachten Technik** – TÜViT-intern
  - mit zusätzlichen ToA-abhängigen Aufgaben für die SU
- **Ergebnisbericht On-Site-Audit**
  - mit Antworten für die vorläufigen Gutachten Recht und Technik
- **Gutachten Recht** – Version 1.0
  - mit dem Prüfergebnis
  - mit Auflagen – Empfehlungen – Hinweisen
- **Gutachten Technik** Version 1.0
  - mit dem Prüfergebnis
  - mit Auflagen – Empfehlungen – Hinweisen

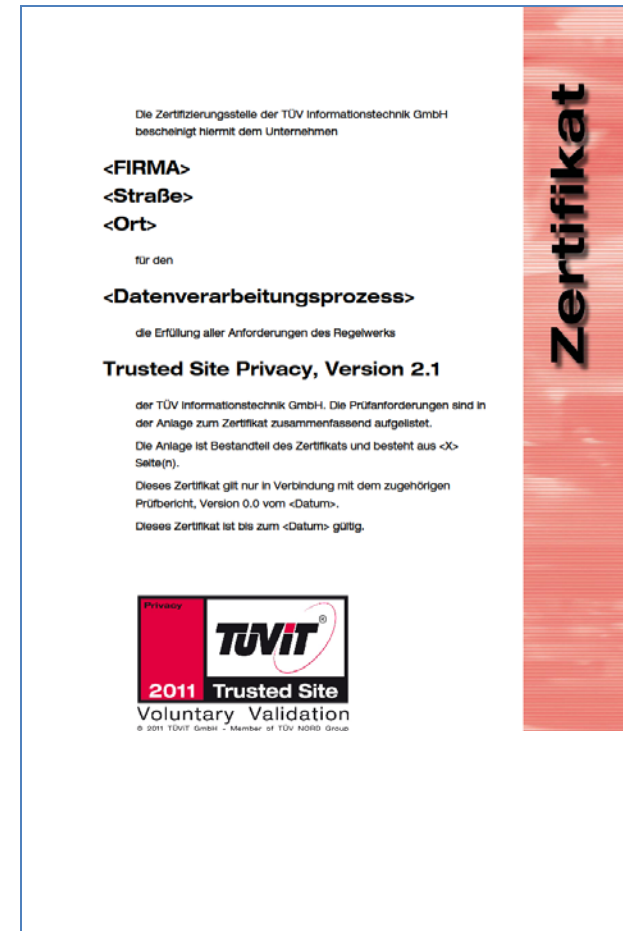
# TSP Privacy Zertifizierung

## Die Zertifizierungsstelle

- **erhält die Ergebnisdokumentation**
  - ToA-Beschreibung – Ergebnisbericht On-Site-Audit – Gutachten Recht – Gutachten Technik
- **prüft die Ergebnisdokumentation hinsichtlich**
  - Erfüllung des Regelwerks
  - Nachvollziehbarkeit
  - Widerspruchsfreiheit
  - Vergleichbarkeit
  - zu erfüllender Auflagen
- **trifft die Zertifikatsentscheidung**
  - Bei Auflagen wird eine Nachprüfung durchgeführt und ein zusätzlicher Auflagen-Prüfbericht erstellt.
- **vergibt das Zertifikat**
  - wenn alle Kriterien erfüllt und keine Auflagen vorhanden sind.

# Trusted Site Privacy Ergebnis

- **ToA**
  - ✓ Beschreibung des ToA
- **Sicherheitstechnische Untersuchung**
  - ✓ Ergebnisbericht On-Site-Audit
- **Audit Recht**
  - ✓ Prüfbericht Recht
- **Audit Technik**
  - ✓ Prüfbericht Technik
- **Zertifizierungsstelle**
  - ✓ Zertifikat, wenn Kriterien erfüllt



# Beispiel: Zertifizierung des E-Postbriefes

## Lessons learned

### ■ Beschreibung des Prüfgegenstands

- alle Datenflüsse incl. Schnittstellen und Datenfelder
- alle IT-Komponenten, Anwendungen, Kommunikationsverbindungen

### ■ Begutachtung der Rechtmäßigkeit

der festgelegten Verarbeitungszwecke (pro Schnittstelle und pro Verarbeitung)

- Benennen der Rechtsgrundlagen
- Bewertung der Einhaltung der Datenschutzgrundsätze und Betroffenenrechte

### ■ Prüfung der technischen Sicherheit

der Komponenten und Anwendungen

### ■ Prüfung der technischen Realisierung der DS-Anforderungen

(z.B. Zweckbindung, vollständige Löschung, Anonymisierung)

- Dokumentenprüfung
- Vor-Ort-Prüfung / On-Site-Prüfung

### ■ Bewertung des organisatorischen Datenschutzes

# Beispiel: Zertifizierung des E-Postbriefes

## Ausgangspunkt Dokumentation – *System-Akte*

Die Dokumentation soll

- **aktuell** vom Inhalt,
- **ausreichend** vom Umfang,
- **vollständig** von der Abdeckung und
- **aufschlussreich** von der Darstellung sein.

# Beispiel: Zertifizierung des E-Postbriefes

## Inhalte der Verfahrensdokumentation I

- Verarbeitungszwecke und die dazugehörige personenbezogene Daten,
- Angabe von Rechtsgrundlagen der Datenverarbeitung samt Begründung (incl. Löschkonzepte),
- Komponenten und Anwendungen,
- Orte der Datenverarbeitung,
- Netzplan,
- die internen und externen Schnittstellen (Beschreibung mit Angabe der Zwecke),
- die vorgesehenen und durchgeführten Datenübermittlungen einschließlich die Empfängerinnen und Empfänger der Daten,
- das Vorliegen einer Datenverarbeitung im Auftrag einschließlich der schriftlichen Vereinbarungen,
- die Maßnahmen zum Erfüllen von Betroffenenrechten.

# Beispiel: Zertifizierung des E-Postbriefes

## Inhalte der Verfahrensdokumentation II

- Dokumentation der **Schutzbedarfsfeststellung**
- Dokumentation der **Risikoanalyse**.
- Dokumentation der technischen und organisatorischen **Sicherheits- und Datenschutzmaßnahmen**.
- Dokumentation der **Tests** der eingesetzten Hard- und Software und der getroffenen Sicherheitsmaßnahmen.

# Inhaltsübersicht

- Einführung
- Datenschutz-Zertifizierung  
*Aktuelle Entwicklungen*
- Was ist ein Zertifikat?
- Was soll und kann eine DS-Zertifizierung leisten?
- Verwendbarkeit der Zertifikate  
*Prüfansätze und Inhalt der Zertifikatsaussagen*
- Zweckgerechte Prüfung  
*Beispiel: TÜVIT TSP- Zertifizierungsverfahren für den E-Postbrief*
- Zusammenfassung

# Mehrwert durch Zertifizierung

## Entscheidende Faktoren

- **Stringente Anwendung** des für den Prüfgegenstand (Produkt, Verfahren, Organisation) **geeigneten Prüfansatzes**
  - ➔ Sicherstellung von
    - **Korrektheit der Prüfaussagen**
    - **Vergleichbarkeit der Zertifikate**
  - ➔ Vermeidung von
    - **gegensätzlichen Prüfergebnissen** (z.B. wenn ein IT-basierter Dienst nur nach dem organisatorischen Ansatz einer Management-Prüfung geprüft wird - ohne Begutachtung der materiell-rechtlichen Zulässigkeit und der technischen Sicherheit in der gesetzlich geforderten Tiefe)
    - **Irreführung**
- Anwendung **sachgerechter Prüfkriterien**
- Transparente Darstellung der Zertifikatsaussagen
- Qualitätsgesichertes Zertifizierungsverfahren

# Datenschutzaudit und -zertifizierung

## Qualitätsmaßstab

- Zweckgerechter Prüfansatz
  - Differenzierung nach Prüfgegenstand (Produkt, Verfahren, Organisation/Managementsystem)
- Anerkannte Prüfkriterien
- Angemessene Prüftiefe und-breite und aussagekräftige Prüfergebnisse
- Transparente Zertifikatsaussagen
- Zweistufiges und qualitätsgesichertes Zertifizierungsverfahren

# Vielen Dank für Ihre Aufmerksamkeit!

**TÜV Informationstechnik GmbH**  
Unternehmensgruppe TÜV NORD

Monika Wojtowicz, LL.M.  
Leiterin Prüfstelle für Datenschutz  
(Recht)

Langemarckstr. 20  
45141 Essen

Telefon: +49 201 8999 – 535  
Telefax: +49 201 8999 – 544  
E-Mail: [m.wojtowicz@tuvit.de](mailto:m.wojtowicz@tuvit.de)  
URL: [www.tuvit.de](http://www.tuvit.de)

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

Langemarckstr. 20  
45141 Essen

Telefon: +49 201 8999 – 582  
Telefax: +49 201 8999 – 555  
E-Mail: [c.sutter@tuvit.de](mailto:c.sutter@tuvit.de)  
URL: [www.tuvit.de](http://www.tuvit.de)