UNIKASSEL
VERSITÄT

Datenschutzzertifizierung: Ende des Dornröschenschlafs?

Potentiale und Erfolgsfaktoren der Zertifizierung als Instrument für eine effektive und grundrechtsorientierte Data Governance

Prof. Dr. Gerrit Hornung, LL.M. / Wiss. Mitarbeiter Marcel Kohpeiß, LL.M.
Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht, Universität Kassel

Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

Jahreskonferenz Forum Privatheit
Berlin, 14. Oktober 2022

Data Governance-Effekte der Zertifizierung

- Zertifizierung als Data Governance-Instrument
- Aktueller Stand in Europa
- Zertifizierbarkeit von Anforderungen jenseits der DSGVO
- Umgang mit offenen Rechtsfragen iRd. Zertifizierung – am Beispiel der Drittstaatenproblematik
- Fazit

Data Governance-Effekte der Zertifizierung

- **Neuordnung der Data Governance-Instrumente** durch die DSGVO
  - Stärkung der klassischen Instrumente (Bußgelder, Anordnungsbefugnisse,…)
  - Stärkung „neuer“ Instrumente (v.a. regulierte Selbstregulierung)

- **Rolle der Zertifizierung in der Data Governance**:
  - (Begrenzte, aber faktisch wirksame) Rechtssicherheit für Verantwortliche, betroffene Personen,… - „Faktor“ / „Gesichtspunkt“ bei Bewertung der DSGVO-Konformität
  - Erleichterung der aufsichtsbehördlichen Tätigkeit
  - Folge (und Hoffnung): Marktanreize zur Entwicklung rechtskonformer Lösungen, d.h.:

- Insbesondere: **europäische Zertifizierung & globale Data Governance**: Zertifizierung als Soft Law-basiertes Tool zum Export europäischer Standards?

Nationales Verfahren

1 Fachprogrammprüfung (AB)

2 Abschluss der Internen Programmprüfung (AB)

3 Informelle Reviewphase (CEH ESG = EDSA Untergruppe)

4 Stellungnahme des Europäischen Datenschutzausschusses (EDSA)

5 Genehmigung der Zertifizierungskriterien (AB)

6 Akkreditierung und Befugniserteilung (DAkkS)

DSGVO-Zertifizierungen

- **GDPR-Certified Assurance-Report based Processing Activities (GDPR-CARPA)**: allgemeine luxemburgische Zertifizierung
  - Genehmigung durch luxemburgische Landesbehörde (CNPD)
  - Akkreditierung von Zertifizierungsstelle(n) ausstehend

- **European Privacy Seal (EuroPriSe)**: allgemeine deutsche Zertifizierung für Auftragsverarbeitungen
  - Genehmigung Zertifizierungskriterien durch LDI NRW (7.10.2022)
  - Veröffentlichung Kriterienkatalog + Akkreditierung Zertifizierungsstelle(n) ausstehend

- **AUDITOR**: vorerst rein nationale deutsche Cloud-Zertifizierung
  - „Informelles“ Reviewverfahren auf EU und nationaler Ebene (LDI NRW als federführende nationale Behörde)
  - Erste Kommentierung des Kriterienkatalogs

Zertifizierbarkeit bereichspezifischer Vorschriften?

- Art. 42 I DSGVO: „nachzuweisen, dass **diese Verordnung**…eingehalten wird“?
- Für enge Auslegung: Wortlaut; einheitliche EU-weite Anwendung nur bei Beschränkung auf DSGVO möglich
- Für weite Auslegung: Zertifizierung (als Data Governance-Instrument) würde erheblich eingeschränkt
  - Zertifikat würde nur Teile der für einen Verantwortlichen geltenden materiell-rechtlichen Anforderungen umfassen
  - Folge: Governance-Effekte (Rechtssicherheit, Marktanreize,…) gemindert / aufgehoben

Beispiele

- Bereichsspezifische, unmittelbar geltende EU-Datenschutznormen (**EU-Verordnungen**)? – zertifizierbar

- Nationale Normen in **Umsetzung bereichsspezifischer EU-Richtlinien** (z.B.: Datenschutz im TTDSG)?
  - Vorrangregel in Art. 95 DSGVO – subsidiäre Geltung der (vielen) DSGVO-Regeln
  - ePrivacy-RL (+ Entwürfe ePrivacy-VO) erwähnen Zertifizierung nicht
  - Sinnvolle : TTDSG zertifizierbar im Rahmen eines modularen Aufbaus – sonst kippt singuläre Spezialvorschrift Zertifizierbarkeit des Gesamtsystems

- **Nationale Normen** in Ausfüllung von **DSGVO-Öffnungsklauseln**?
  - Klauseln = Teil „dieser Verordnung“ – Zertifizierung in nationalen (!) Programmen möglich
  - Problem: föderale Diversität – Modularisierung pro Bundesland? Kumulation der Anforderungen (Widerspruchsfreiheit)? „Anpassbarkeit an Landesrecht“ als Zertifizierungskriterium?

Problemstellung

- Grundproblem: viele **generische Anforderungen** der DSGVO – viele Rechtsstreitigkeiten

- Lösung / Verarbeitung **im Zertifizierungsprozess**? An welcher Stelle? Durch wen?

- **Beispiel: Drittlandsübermittlung** (USA)
  - Kein (allgemeines) angemessenes Schutzniveau (v.a.: Befugnisse der Nachrichtendienste + fehlender Rechtsschutz)
  - EuGH: Safe Harbor + Privacy Shield verstießen gegen Art. 7, 8 und 47 EU-GRCh – Folgen für Data Privacy Framework (Presedential Order vom 7.10.) offen
  - Weitere Garantien:
    a) EuGH: Pflicht zu Transfer-Impact-Assessment (TIA) bei Standard Contractual Clauses (SCCs)
    b) EDSA: TIA bei allen weiteren Garantien erforderlich; ggf. technische Maßnahmen nötig (konkret: Anonymisierung / Pseudonymisierung; Schlüssel verbleibt in EU)

1. Lösungsansatz für Zertifizierung

- Art. 42 II iVm. Art. 46 I lit. f DSGVO – **Zertifizierung des Datenimporteurs** im Drittland

- **Anforderungen (EDSA-Vorgaben)**:
  - Leitlinien 01/2018 (Zertifizierung + Ermittlung von Zertifizierungskriterien)
  - Leitlinien 07/2022 (Zertifizierung als Übermittlungstool)
  - Empfehlung 01/2020 (Maßnahmen zur Ergänzung von Übermittlungstools):
    a) TIA: Importeur + Exporteur, wenn sich darauf stützen will
    b) Kein gleichwertiges Schutzniveaus: **(technische) Maßnahmen** erforderlich
    c) Konkret USA letztlich: **Anonymisierung / Pseudonymisierung** (vorbehaltlich neuer Angemessenheitsbeschluss)

- **Ergebnis**:
  - Zertifizierung kann iRv. Art. 46 I lit. f DSGVO als Garantie genutzt werden
  - Fehlende Angemessenheit aber nur durch Maßnahmen im Kriterienkatalog lösbar
  - Probleme der Kontrolle + Durchsetzung im Drittland bislang völlig offen

2. Lösungsansatz für Zertifizierung

- Integration der Art. 44 ff. DSGVO in die **Zertifizierung des Datenexporteuers** in der EU – Optionen:

- **Kriterienkatalog als reine Wiedergabe** der Art. 44 ff. DSGVO?
  - Folge: Prüfung durch Zertifizierungsstellen
  - Weiterhin Rechtsunsicherheit / offener Rechtsbruch iRv. Art. 46 I DSGVO?
  - ABs müssen Standards setzen (Überprüfung von Zertifizierungsstellen + Zertifizierungen)

- **Kriterienkatalog als Konkretisierung** der Art. 44 ff. DSGVO?
  - Übernahme der EuGH-Anforderungen – Umgang mit (potentiell zweifelhaftem, sofort gerichtlich angegriffenen) Angemessenheitsbeschluss zum Data Privacy Framework?
  - EDSA-Anforderungen (Anonymisierung / Pseudonymisierung)
    a) Übernahme – weitgehender Ausschluss von US-Services?
    b) Keine Übernahme – gerichtliche Klärung der Reichweite?
  - Ausschluss der Übermittlung
    a) In alle Länder außerhalb der EU?
    b) In Länder mit (trotz Angemessenheitsbeschluss) zweifelhaftem Datenschutzniveau?

Fazit

- Potentiale der Zertifizierung zur effektiven und grundrechtsorientierten Data Governance erkennbar – aber (bei weitem) nicht ausgeschöpft
- Effektive + wirksame Zertifizierung setzt zumindest im Grundsatz Zertifizierbarkeit bereichsspezifischer Anforderungen voraus
- Unbestimmter Charakter vieler DSGVO-Normen ist allgemeines Governance-Problem
  - Im Rahmen der Zertifizierung nur eingeschränkt lösbar
  - Maßgeblicher Einfluss bei ABs und Gerichten
- Zertifizierung als möglicher Baustein einer transatlantischen Daten Governance – aber bis auf weiteres überlagert durch Data Privacy Framework

Datenschutzzertifizierung: Ende des Dornröschenschlafs?

Potentiale und Erfolgsfaktoren der Zertifizierung als Instrument für eine effektive und grundrechtsorientierte Data Governance

Prof. Dr. Gerrit Hornung, LL.M. / Wiss. Mitarbeiter Marcel Kohpeiß, LL.M.
https://www.uni-kassel.de/go/hornung