UNIKASSEL VERSITÄT

ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

# Dynamische Zertifizierung:

# Der Weg zum verordnungskonformen Cloud Computing

Johanna M. Hofmann, LL.M.
j.hofmann@uni-kassel.de
+49 / 561 / 804-6085

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

# Aufbau

1. Datenschutz beim Cloud Computing
2. Zertifizierung als Nachweis der Datenschutzkonformität
3. Dynamische Zertifizierung
4. Regelungsempfehlungen: Was? Wer?
5. Fazit

## Auftragsverarbeitung

- (str.) Rechtsgrundlage: Art. 6 DS-GVO
- Verantwortlichkeit des Cloud-Kunden
- Pflicht zur Zusammenarbeit mit Anbietern, die hinreichende Garantien für die Verordnungskonformität bieten: Art. 28 Abs. 1
- Pflicht beider zur Einhaltung der Datensicherheit
  - Monitoring zur Überwachung der Wirksamkeit
- Nachweis, sonst drohen

Bußgelder

Schadensersatz

→ **kontrollieren und anweisen**

# Probleme beim Cloud Computing

Informationsasymmetrie

Technik | Tatsachen | Recht

Dynamik

→ **Kontrolle ist nicht realisierbar**

## Zertifizierung

- Vertrauensverlagerung
- Faktor beim Nachweis
- Wettbewerb

## Probleme herkömmlicher Verfahren:

- Mangelnde Vergleichbarkeit
- Momentaufnahme
- Suggeriert Sicherheit
- Lauterkeitsrechtliche Bedenken

Transparenz

Dynamische Zertifizierung

= **Kontinuierliche, möglichst automatisierte Zertifizierung**

## Stand der Forschung:

- **Verfahren muss entwicklungsoffen konzipiert sein**
- **Beteiligte:** Zertifizierer, Cloud-Anbieter, Zertifizierungsdienst-Anbieter, Auditor
- **Use Cases:** Verfügbarkeit, Identity-Management, Datenlokation
- **Herausforderung:** Schließen der Semantiklücke
- **Verfahrenskomponenten:** Automatisierte Messungen (invasiv/nicht invasiv), Informationsregeln und Reaktionszeiträume
- **Grenzen:**

Technik | Tatsachen | Recht

NGCert

ngcert.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

provet

UNIKASSEL VERSITÄT

## Wie steht die DS-GVO zur Dynamik?

1. Allgemein:
   - technikoffen
   - unbestimmte Rechtsbegriffe
2. Auftragsverarbeitung:
   - Weisungshoheit
   - Art. 28: kontinuierliche Überprüfung und Anpassung
   - Art. 24: TOM  werden „erforderlichenfalls überprüft und aktualisiert“
3. Zertifizierungsverfahren:
   - Rahmenbedingungen: Beurteilungsspielraum der Zertifizierer
   - Kommissionsbefugnisse

# Regulierung

## Art. 42 DS-GVO

- Definitionen
- Rollentrennung
- Mitwirkung bei der Zertifizierung
- „Transparentes“ Verfahren
- Verfahren zur Überprüfung

## Art. 43 DS-GVO

- Fachkenntnis
- Interessenkonflikt / Unabhängigkeit (negativ)
- Verfahren zur Erteilung und zum Widerruf

# Wer sollte Dynamik regeln?



**EU**

- Gesetzgeber
- Kommission
- Ausschuss

**D**

- Gesetzgeber (Bund)
- Gesetzgeber (Land)
- Aufsichts-behörden

# EU-Kommission


## 1. Delegierte Rechtsakte

- Anforderungen an Prüfkriterienkataloge konkretisieren
  - Konkretheit (Automatisierbarkeit)
  - Aktualität (Dynamik)
- Begriffe definieren, abgrenzen und konkretisieren
- Anforderungen an das Verfahren festsetzen

## 2. Durchführungsrechtsakte

- Feststellen, dass konkrete dynamische Messmethoden zum Erlasszeitpunkt dem Stand der Technik entsprechen
- Förderung und Anerkennung (dynamischer) Zertifizierungsverfahren

## 3. Standardvertragsklauseln

- Formblätter


# Rollentrennung innerhalb der Aufsichtsbehörde

- Unabhängigkeit gefährdet
- Kompetenz des Bundes
  - Mitgliedsstaatlicher Verwaltungsaufbau
  - gegenüber den Ländern
    - Konkurrierend bei wirtschaftlicher Tätigkeit
    - Konkretisierung von EU-Recht für Bundesbehörden
    - Konkretisierung von EU-Recht für Landesbehörden
      - Bedürfnis nach einheitlicher Regelung
      - Abweichungskompetenz der Länder


## Verfahren für die Überprüfung, den Widerruf oder die Erteilung von Zertifizierungen durch private Stellen

- Kompetenz
- Attraktivität einer Zertifizierung steigt mit Abnahme ihrer Anforderungen
- Race-to-the-Bottom
- Vereinheitlichung
- Vergleichbarkeit
- Dynamik


## Kriterienkatalog / Empfehlungen / Standardvertragsklauseln

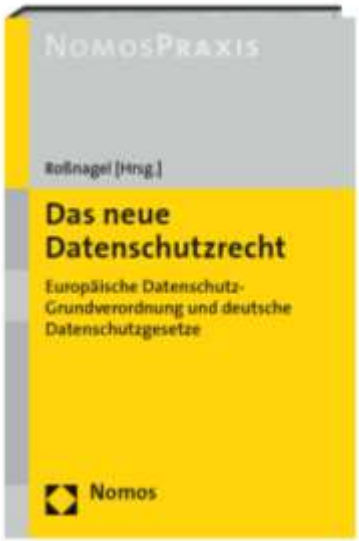
1. Kriterienkatalog
   - Kohärenzverfahren durch andere Aufsichtsbehörden
   - Wirtschaftlich motiviertes Gegeneinander-Ausspielen
   - Jedes Verfahren? → Kompetenz läuft faktisch leer
   - Dennoch: dringend Rechtssicherheit

2. Empfehlungen und Richtlinien aussprechen: Wann kann ein Verfahren als „Faktor“ angesehen werden, wann nicht?

3. Standardvertragsklauseln

# Dynamischer Gegenstand → dynamischer Nachweis

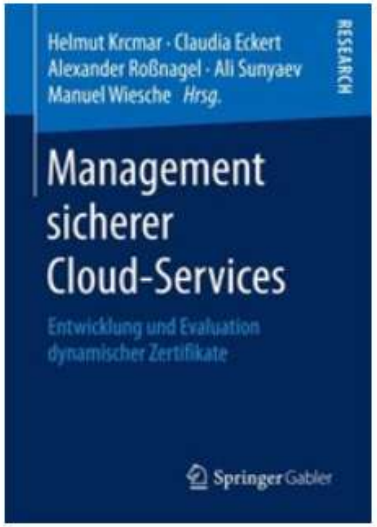
- Dynamische Zertifizierung
  - verhilft dem Cloud Computing zur Rechtmäßigkeit
  - verbreitert die Tatsachenbasis: Transparenz
  - räumt lauterkeitsrechtliche Bedenken aus
  - bedarf allerdings der Konkretisierung
    - Regulierung
    - Weiteren Forschung




**Das neue Datenschutzrecht**
Europäische Datenschutz-Grundverordnung
und deutsche Datenschutzgesetze
Herausgegeben von Prof. Dr. Alexander Roßnagel
*2017, ca. 400 S., geb., ca. 58,– €*
*ISBN 978-3-8487-4411-4*
*Erscheint ca. Dezember 2017*
*nomos-shop.de/30426*

**Ankündigung**

**Ankündigung**




Krcmar / Eckert / Roßnagel / Sunyaev / Wiesche
**Management sicherer Cloud-Services**
Entwicklung und Evaluation dynamischer Zertifikate

**Jetzt vorbestellen!**

Inhaltsverzeichnis

provet
UNIKASSEL VERSITÄT

UNIKASSEL VERSITÄT

ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

# Vielen Dank!

Johanna M. Hofmann, LL.M.
j.hofmann@uni-kassel.de
+49 / 561 / 804-6085

provet
Projektgruppe verfassungsverträgliche Technikgestaltung