Prof. Dr. Georg Borges
Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie

UNIVERSITÄT DES SAARLANDES

Auftragsdatenverarbeitung und Zertifizierung nach der DSGVO

17. März 2016, Köln

a | i3

Arbeitsgruppe **Identitätsschutz im Internet**

ADV – Grundlage moderner DV

ADV – Grundlage moderner DV

Auftragsdatenverarbeitung (ADV)
= Verarbeitung (personenbezogener) Daten für Dritte

- Beispiel: **Hosting**
  - nicht:
    - Putzen eines Büros
    - Austragen eines Briefes
  - streitig: Wartung einer DV-Anlage

ADV – Grundlage moderner DV

Merksatz

In der digitalen Gesellschaft gilt:

Keine **DV** ohne **A**uftrags **DV**

Rechtliche Grundlagen der Auftragsdatenverarbeitung

- Datenschutzrichtlinie
  - Art. 17
- Bundesdatenschutzgesetz (BDSG)
  - § 3 VIII 3
    - ADV als Grundlage für DV-Dienste
  - § 11
    - Voraussetzungen für DV
- Datenschutz-Grundverordnung (DSGVO)
  - Art. 26

Grundsätze der Auftragsdatenverarbeitung

Die rechtliche Struktur der Auftragsdatenverarbeitung

Quelle: de.wikipedia / Etmot– CC-BY-SA

Auftraggeber

Auftragnehmer

Kunde

Grundsätze der Auftragsdatenverarbeitung

- Auftraggeber = verantwortliche Stelle
  - Adressat der datenschutzrechtlichen Pflichten

- Auftragnehmer (Dienstleister)
  - Bindung an Auftraggeber
  - eingeschränkter Adressat des Datenschutzes

- Verhältnis Auftraggeber – Auftragnehmer
  - vertragliche Grundlage
  - Weisungsgebundenheit des Auftragnehmers
  - Überwachungspflicht des Auftraggebers

Die Regelung der ADV in der DSGVO

- Terminologie
  - Auftragsdatenverarbeitung / Auftragsverarbeitung
  - Auftraggeber:
    Controller / Der für die Verarbeitung Verantwortliche (VV)
  - Auftragnehmer:
    Processor / Auftragsverarbeiter (AV)
  - Auftragsdatenverarbeitung:
    Processing / Auftragsverarbeitung

- Regelung: Artt. 26 – 27 DSGVO

Die Regelung der ADV in der DSGVO

- Art. 26 DSGVO-E
  - Auswahl von AV mit Gewähr für TOM, Abs. 1
  - Zustimmungserfordernis für UAV, Abs. 1a
  - vertragliche Grundlage, Abs. 2
  - Anforderungen an Unterauftragsverarbeitung, Abs. 2a
  - Gewähr durch Zertifizierung / Kodizes, Abs. 2aa
  - Standardvertragsklauseln, Abs. 2ab
  - Ermächtigung Kommission, Abs. 2b
  - Form, Abs. 3

Die Regelung der ADV in der DSGVO

- Art. 27 DSGVO
  - Weisungsgebundenheit des AV

- Art. 28 DSGVO
  - umfassende Dokumentationspflicht > 250 Arbeitnehmer
  - für VV, Abs. 1
  - für AV, Abs. 2

Probleme der ADV und DSGVO

- Form des ADV-Vertrags
  - BDSG: Schriftform i.S.v. § 126 BGB (h.M.)
  - DSGVO: Schriftlichkeit

- Überwachung des AV
  - BDSG: Überzeugung von Einhaltung der TOM
  - DSGVO: Gewähr für TOM

Überwachungserfordernis und moderne DV

Art. 17 Abs. 4 Datenschutzrichtlinie

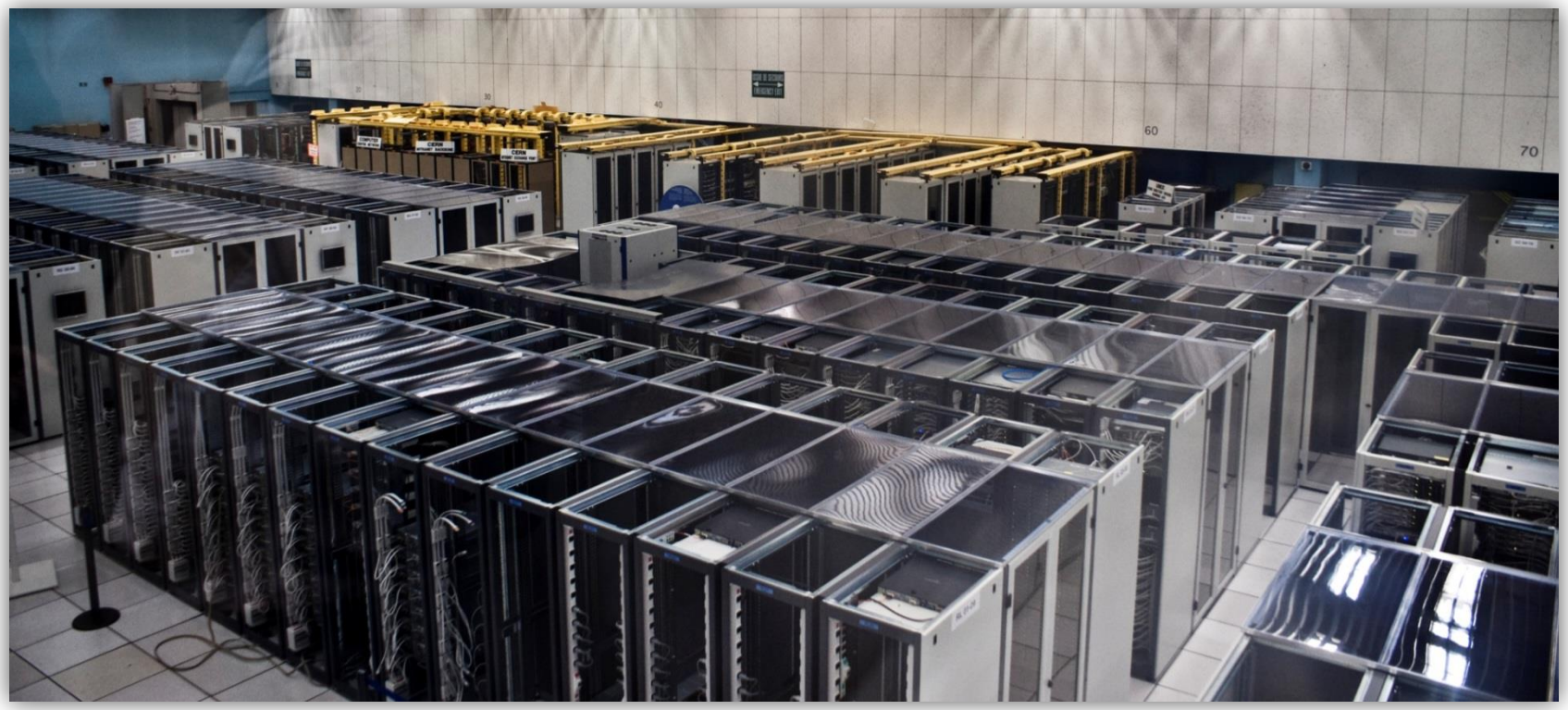
(2) Die Mitgliedstaaten sehen vor, daß der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; **der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.**

Überwachungserfordernis und moderne DV

§ 11 Abs. 2 S. 4 BDSG

Der **Auftraggeber hat sich** vor Beginn der Datenverarbeitung und sodann regelmäßig **von der Einhaltung** der beim Auftragnehmer getroffenen **technischen und organisatorischen Maßnahmen zu überzeugen.**

Überwachungserfordernis und moderne DV



Quelle: Florian Hirzinger – CC-BY-SA

Überwachungserfordernis und moderne DV

Quelle: Philippe Heckel – CC-BY

Überwachungserfordernis und moderne DV

Datenschutz als Prüftourismus?

Quelle: Vladislav Bezrukov – CC-BY (bearbeitet)

Überwachungserfordernis und moderne DV

Lösung für Überzeugungspflicht: Zertifizierung

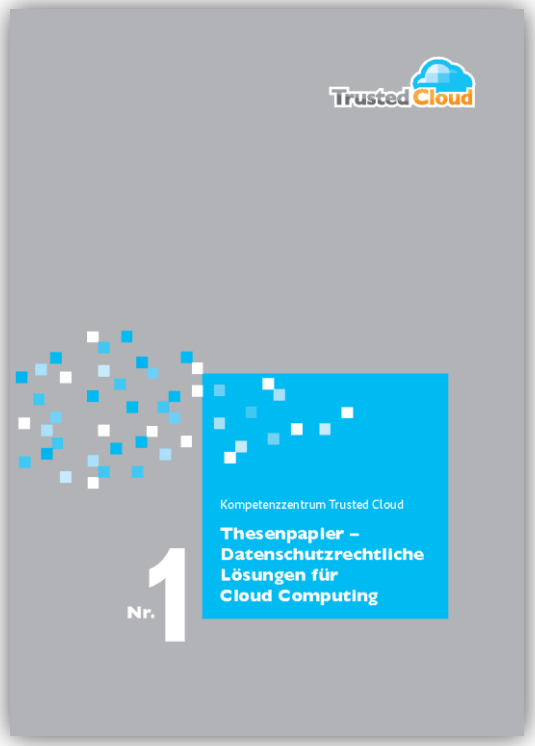
These 5

Das wesentliche Problem des Kontrollerfordernisses kann gelöst werden, wenn die Kontrolle durch den Auftraggeber durch das von einem unabhängigen Dritten erstellte Testat ersetzt werden kann, das die Durchführung der Kontrolle im gesetzlich angeordneten Umfang bescheinigt. Die Ersetzbarkeit der Überprüfung durch ein Testat ist gesetzlich festzuschreiben.

AG Rechtsrahmen des Cloud Computing

- Arbeitsgruppe „Rechtsrahmen des Cloud-Computing“
- Leitung: Prof. Dr. Georg Borges

- Mitglieder der Arbeitsgruppe
  - Vertreter der Trusted Cloud-Projekte
  - externe Experten
    - Datenschutzbehörden
    - Verbänden, Cloud-Anbietern und Cloud-Nutzern
    - Rechtsanwaltschaft
    - Wissenschaft



- Konzept zur Zertifizierung für Cloud-Dienste

Zertifizierung von Cloud-Diensten

- Trusted Cloud
  - Technologieprogramm des BMWi (2011- 2015)
  - Förderung von Projekten
  - Begleitforschung

- Begleitforschung
  - AG Rechtsrahmen des Cloud Computing
  - Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

- November 2013 – April 2015
- Leitung: Prof. Dr. Georg Borges

- Projektbeteiligte
  - 7 Datenschutzbehörden
  - 3 Verbände
  - 4 Cloud-Anbieter
  - 2 Rechtsanwaltssozietäten
  - 2 Anbieter von IT-Prüfungen
  - DIN, Stiftung Datenschutz

Designed by freepik.

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

- Beobachterstatus
  - Europäische Kommission
  - Bundesministerium des Innern
  - Bundesamt für Sicherheit in der Informationstechnik

Designed by freepik.

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

- Beobachterstatus
  - Europäische Kommission
  - Bundesministerium des Innern
  - Bundesamt für Sicherheit in der Informationstechnik

Designed by freepik.

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

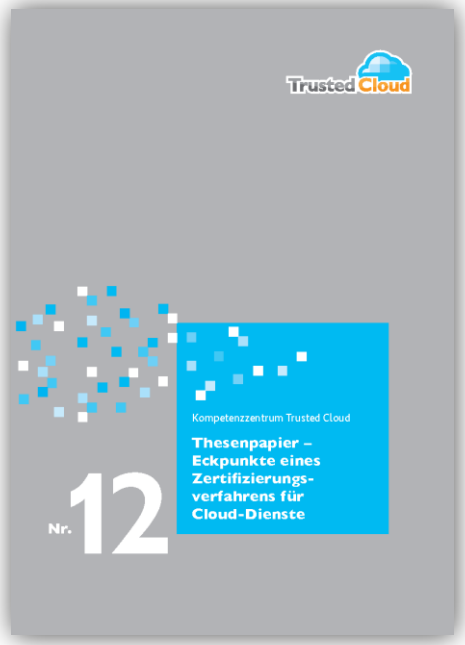
- Arbeitsauftrag
  - Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)
  - Konzepte zu zentralen Aspekten der Zertifizierung
  - Untersuchungen zum Verfahren der datenschutzrechtlichen Zertifizierung

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

- Prüfanforderungen
  - Maßstab: Gesetz (BDSG / DSGVO)
  - Herausforderung: Umsetzung zu prüffähigen Anforderungen
  - Entwicklung eines Prüfkatalogs (Datenschutz-Standard)
  - Lösung:
    Trusted-Cloud Datenschutz-Profil für Cloud Dienste (TCDP)
  - Basis: ISO/IEC 27018 und ISO/IEC 27002

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 1“

- Zertifizierungsverfahren
  - Herausforderung: Qualität des Verfahrens
  - Lösung: Verfahrensgrundsätze und Haftung



Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 2“

- Zeitraum: September 2015 – April 2016
- TÜV Informationstechnik GmbH (TÜViT)
  - Projektleitung
  - Pilot-Prüfung und -Zertifizierung ausgewählter Dienste
- Prof. Dr. Georg Borges
  - Wissenschaftliche Leitung
  - Konzeptionelle Aspekte der Datenschutz-Zertifizierung
- Europäische EDV-Akademie des Rechts gGmbH (EEAR)
  - Konzeptionelle Aspekte der Datenschutz-Zertifizierung
  - Projektbüro

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste – Phase 2“

- Pilot-Zertifizierung von Cloud-Diensten
- Überprüfung und Weiterentwicklung des TCDP
- Verfahren der Datenschutz-Zertifizierung
- Die europäische Dimension der Zertifizierung

Vorteile der Zertifizierung

- Dienstleister (z.B. Cloud-Anbieter)
  - Nachweis der Datenschutz-Compliance

- Kunde (z.B. Cloud-Nutzer)
  - Erfüllung der Überwachungspflicht


Trusted Cloud
Übergabe der ersten Zertifikate nach
Trusted Cloud Datenschutz-Profil für Cloud-Dienste
CeBIT 2016, 17. März
Bundesministerium für Wirtschaft und Energie

Zertifizierung und DSGVO

Zertifizierung als grundlegender Ansatz

- Art. 22 Abs. 2a: TOM
- Art. 26 Abs. 2aa: TOM
- Art. 30 Abs. 2a: TOM
- Art. 42: Drittstaatenübermittlung

Art. 26 Abs. 2aa DSGVO

2aa. Die Einhaltung […]eines genehmigten Zertifizierungsverfahrens gemäß Artikel 39 durch den Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 2a nachzuweisen.

Regelung der Zertifizierung, Art. 39, 39a DSGVO

- Zertifizierung durch akkreditierte Zertifizierungsstellen, Art. 39a Abs. 1

- Verantwortlichkeit der Zertifizierungsstelle für Bewertung, Art. 39a Abs. 4

- Ermächtigungsgrundlage für Kommission betr. Standards, Art. 39a Abs. 8

Fazit

- AV in DSGVO ähnlich wie BDSG
- neu: große Bedeutung der Zertifizierung

Vielen Dank für Ihre Aufmerksamkeit!

Prof. Dr. Georg Borges

georg.borges@uni-saarland.de

it-recht.uni-saarland.de

www.rechtsinformatik.saarland