Prof. Dr. Georg Borges
Lehrstuhl für Bürgerliches Recht,
Rechtstheorie und Rechtsinformatik

UNIVERSITÄT
DES
SAARLANDES

Cloud Computing und Datenschutz

IT-Themenabend, 10. November 2015

a | i3
Arbeitsgruppe **Identitätsschutz im Internet**

OneDrive Download | Plans | How-to | Business | Blogs ∨ Sign up Sign in

One place for everything in your work life

Save your work files to OneDrive for Business so they're always with you.

Store

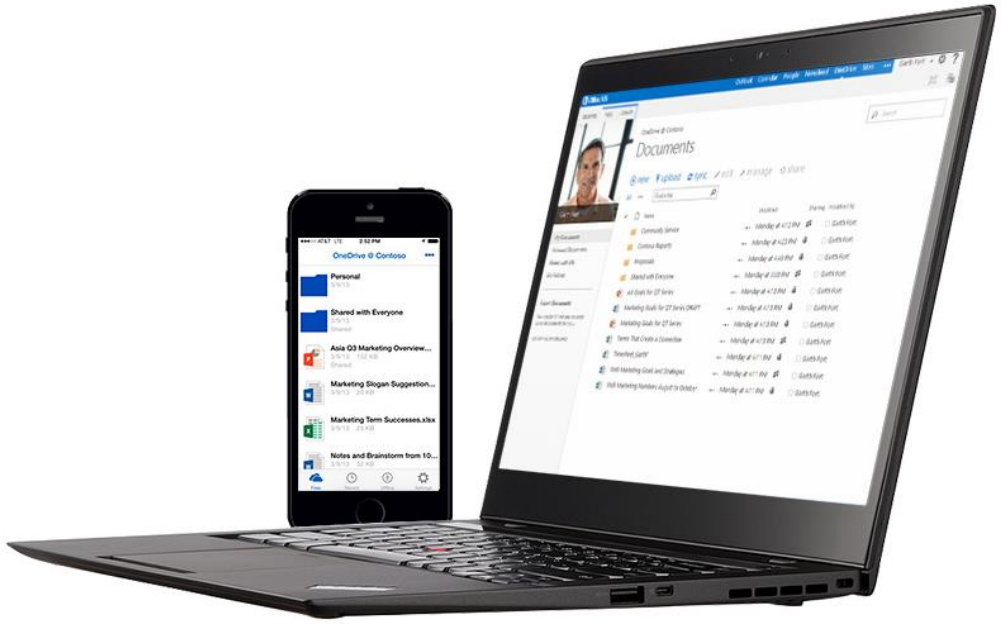
Securely store all your files and share them with coworkers. Each user gets 1 TB of storage.

Sync

Sync files across devices and access them anywhere, even when you're offline.

Search

Find the files you need in seconds with simple search. Or use Office Delve to discover new relevant content.



Prof. Dr. Georg Borges

- Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtstheorie und Rechtsinformatik, Universität des Saarlandes
- Geschäftsführender Direktor, Institut für Rechtsinformatik, Richter am Oberlandesgericht Hamm a.D.
- Sprecher des Vorstands, Arbeitsgruppe Identitätsschutz im Internet (a-i3)
- Mitglied des Vorstands, EDV-Gerichtstag, e.V.
- Mitglied des Verwaltungsrats, Stiftung Datenschutz
- Mitglied CISPA, HGI

Das Institut für Rechtsinformatik

INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

- Struktur
  - 3 juristische Lehrstühle der Rechts- und Wirtschafts-wissenschaftlichen Fakultät
  - juris-Stiftungsprofessur für Rechtsinformatik
  - Kooperation mit Uni Luxemburg (Prof. Cole)
- Themenfelder
  - IT-Recht
  - eJustice, eGovernment
  - Datenschutz
  - IT-Sicherheit
  - Rechtsinformatik
- Informationen: www. rechtsinformatik.saarland

Gliederung

I. **Was ist Cloud Computing?**

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

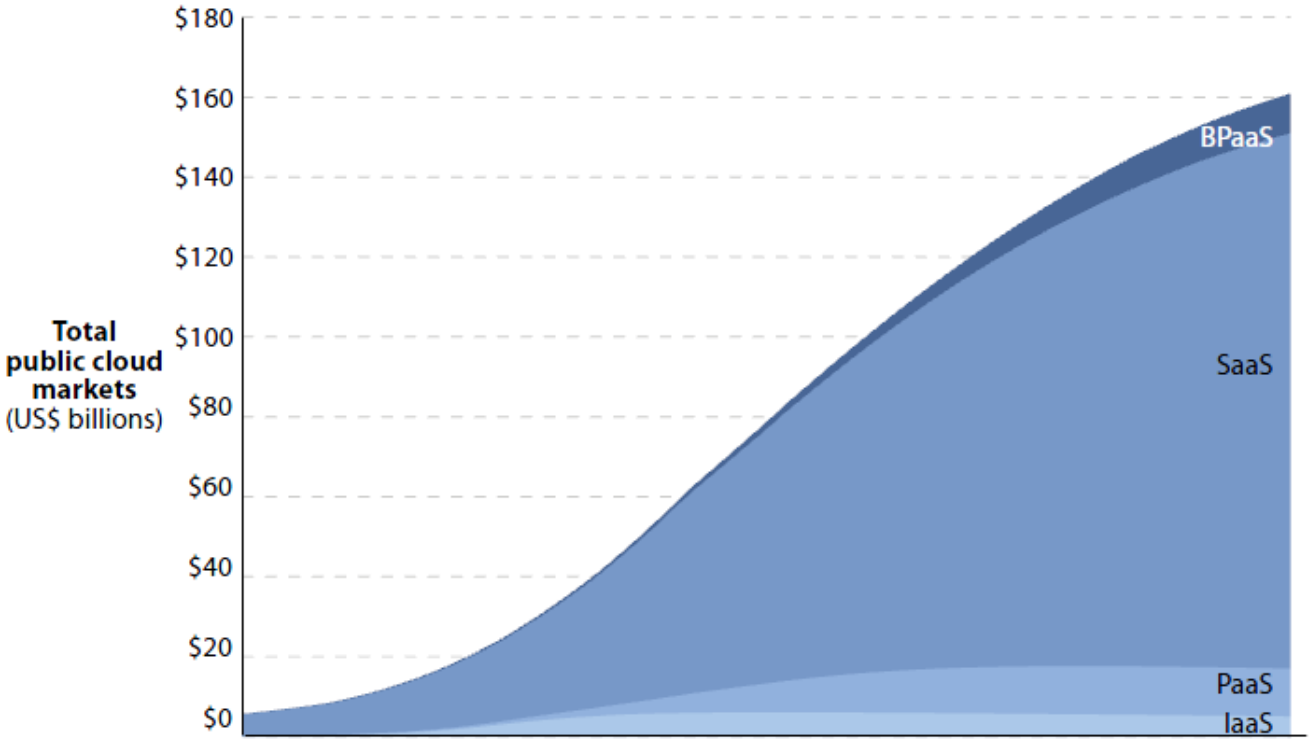
IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

I. Was ist Cloud Computing?



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BPaaS ($)	0.15	0.23	0.35	0.53	0.80	1.26	1.95	2.93	4.28	6.00	7.66	9.08	10.02
SaaS ($)	5.56	8.09	13.40	21.21	33.09	47.22	63.19	78.43	92.75	105.49	116.39	125.52	132.57
PaaS ($)	0.05	0.12	0.31	0.82	2.08	4.38	7.39	9.80	11.26	11.94	12.15	12.10	11.91
IaaS ($)	0.06	0.24	1.02	2.94	4.99	5.75	5.89	5.82	5.65	5.45	5.23	5.01	4.78

I. Was ist Cloud Computing?

Definition des Cloud Computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST Definition of Cloud Computing

I. Was ist Cloud Computing?

Die Bedeutung des Cloud Computing für Internet-Nutzer

ubuntu one

iCloud

Google Drive

Dropbox

I. Was ist Cloud Computing?

Die rechtliche Struktur des Cloud Computing

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

Cloud-Nutzer

Cloud-Anbieter

Kunde

I. Was ist Cloud Computing?

Die rechtliche Struktur des Cloud Computing

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

Cloud-Nutzer

Cloud-Anbieter

Quelle: Klaus Böhringer– CC-BY-SA

I. Was ist Cloud Computing?

Herausforderungen des Cloud Computing – Datensicherheit

- Herausforderung im Cloud Computing: Schutz von Daten
  - vor Datenverlust
  - Einsichtnahme/Verwendung durch unbefugte Dritte

Quelle: pixelio.de / Antje Delater

I. Was ist Cloud Computing?

Cloud als standardisierte Dienstleistung

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST Definition of Cloud Computing

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

II. Cloud Computing und Datenschutz

Rechtliche Grundlagen

- Bundesdatenschutzgesetz
- Landesdatenschutzgesetze / Bereichsdatenschutz (z.B. SGB)
- Sonderregelungen (TMG, TKG)
- Datenschutz-Richtlinie
  - **Richtlinie 95/46/EG des Europäischen Parlaments** und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

II. Cloud Computing und Datenschutz

Rechtliche Grundlagen

- künftig: Datenschutz-Grundverordnung
  - **Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM/2012/011 endgültig – 2012/0011 (COD)

- Leitlinie der Aufsichtsbehörden
  - *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe Cloud Computing, Version 2.0, Stand 09.10.2014

II. Cloud Computing und Datenschutz

Datenschutz als Hemmnis für Cloud Computing?

- „Das derzeit noch bestehende Grundprinzip der ‚freien' Cloud genügt **nicht den Anforderungen des modernen Datenschutzes** […]"
  - Thilo Weichert, DuD 2010, 679, 687

- „Unseres Erachtens **beschränken datenschutzrechtliche Regelungen** daher in erheblichem Maße den **Anwendungsbereich des Cloud Computing**."
  - Nägele/Jacobs, ZUM 2010, 281, 290

II. Cloud Computing und Datenschutz

Cloud-Struktur

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

Cloud-Nutzer

Cloud-Anbieter

Kunde

II. Cloud Computing und Datenschutz

Datenschutzrechtliche Rechtfertigung des Cloud Computing

- Grundsatz: „Verbot mit Erlaubnisvorbehalt“
- Rechtfertigung für Datenverarbeitung des Cloud-Nutzers (verantw. Stelle)
  - Einwilligung des Betroffenen
  - Gesetzliche Erlaubnis

II. Cloud Computing und Datenschutz

Datenschutzrechtliche Rechtfertigung des Cloud Computing

- Rechtfertigung für Datenübermittlung an Cloud-Anbieter
  - Einwilligung des Betroffenen
  - Gesetzliche Erlaubnis
  - Auftragsdatenverarbeitung

- Rechtfertigung für Datenverarbeitung durch Cloud-Anbieter
  - Einwilligung des Betroffenen
  - Gesetzliche Erlaubnis
  - Auftragsdatenverarbeitung

II. Cloud Computing und Datenschutz

Datenschutzrechtliche Rechtfertigung des Cloud Computing

- Rechtfertigung des Cloud Computing nach § 28 BDSG

§ 28 BDSG
Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. ...
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
3. ...

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

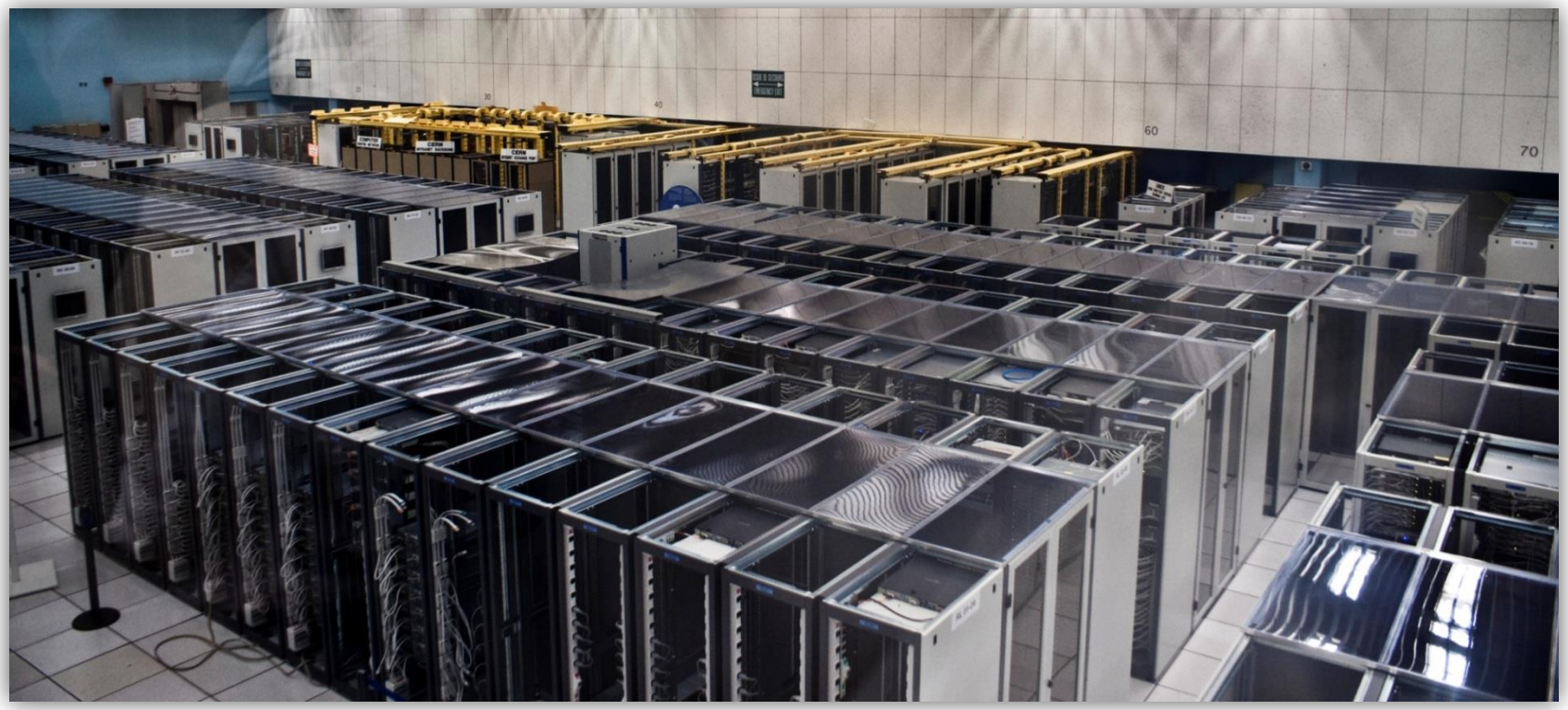
V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

III. Cloud Computing und Auftragsdatenverarbeitung

Charakteristika der Auftragsdatenverarbeitung



Quelle: Florian Hirzinger – CC-BY-SA

III. Cloud Computing und Auftragsdatenverarbeitung

Charakteristika der Auftragsdatenverarbeitung

- Zulässigkeit der Auftragsdatenverarbeitung ohne Einwilligung des Betroffenen
- Verantwortlichkeit des Auftraggebers gegenüber dem Betroffenen
- eingeschränkte Verantwortlichkeit des Auftragnehmers
- vertragliche Bindung des Auftragnehmers an den Auftraggeber
- Weisungsrecht des Auftraggebers
- Pflicht zur Kontrolle des Auftragnehmers durch den Auftraggeber

III. Cloud Computing und Auftragsdatenverarbeitung

Cloud Computing und Auftragsdatenverarbeitung

- neue Bereiche der Trennung von inhaltlicher und technischer Datenverarbeitung
  - private Datenverarbeitung
  - Datenverarbeitung kleiner Unternehmen
  - Belastungsspitzen

CLOUDwerker

Quelle: Flickr / richardmasoner – CC-BY-SA

III. Cloud Computing und Auftragsdatenverarbeitung

Cloud als standardisierte Dienstleistung

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with **minimal management effort** or service provider interaction."

NIST Definition of Cloud Computing

III. Cloud Computing und Auftragsdatenverarbeitung

Anforderungen an Vertragsinhalt, § 11 Abs. 2 BDSG

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

III. Cloud Computing und Auftragsdatenverarbeitung

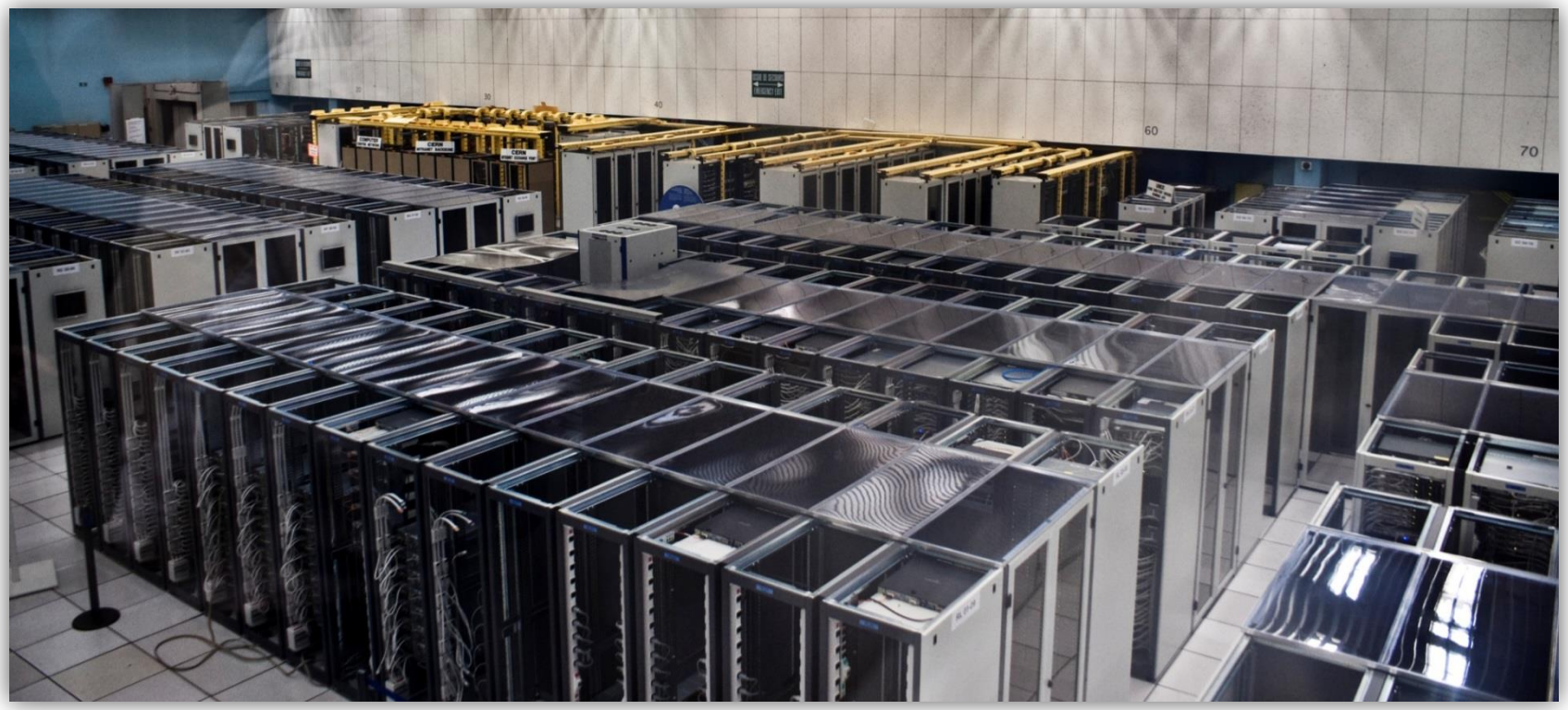
Anforderungen an Vertragsinhalt, § 11 Abs. 2 BDSG

- Schriftform des Vertrags

Quelle: Bundesarchiv – CC-BY-SA

III. Cloud Computing und Auftragsdatenverarbeitung

Herausforderungen des Cloud Computing – Datensicherheit



Quelle: Florian Hirzinger – CC-BY-SA

III. Cloud Computing und Auftragsdatenverarbeitung

Herausforderungen des Cloud Computing – Datensicherheit

Quelle: Philippe Heckel – CC-BY

III. Cloud Computing und Auftragsdatenverarbeitung

Kontrolle des Auftragnehmers durch Auftraggeber

Quelle: Vladislav Bezrukov – CC-BY (bearbeitet)

III. Cloud Computing und Auftragsdatenverarbeitung

Zwischenergebnis

- gesetzliche Regelung der Auftragsdatenverarbeitung nur teilweise geeignet
- Schriftformerfordernis überzogen
- Kontrollpflicht problematisch

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

IV. Lösung: Zertifizierung

Ersetzung der eigenen Kontrolle durch ein Zertifikat

- Rechtspolitischer Vorschlag:
  Modifikation der Überwachungspflicht
  - AG Rechtsrahmen des Cloud Computing
  - Arbeitsgruppe im Kompetenzzentrum Trusted Cloud
  - Experten aus Wirtschaft und Wissenschaft, Datenschutz
  - rechtspolitisches Thesenpapier

Trusted Cloud

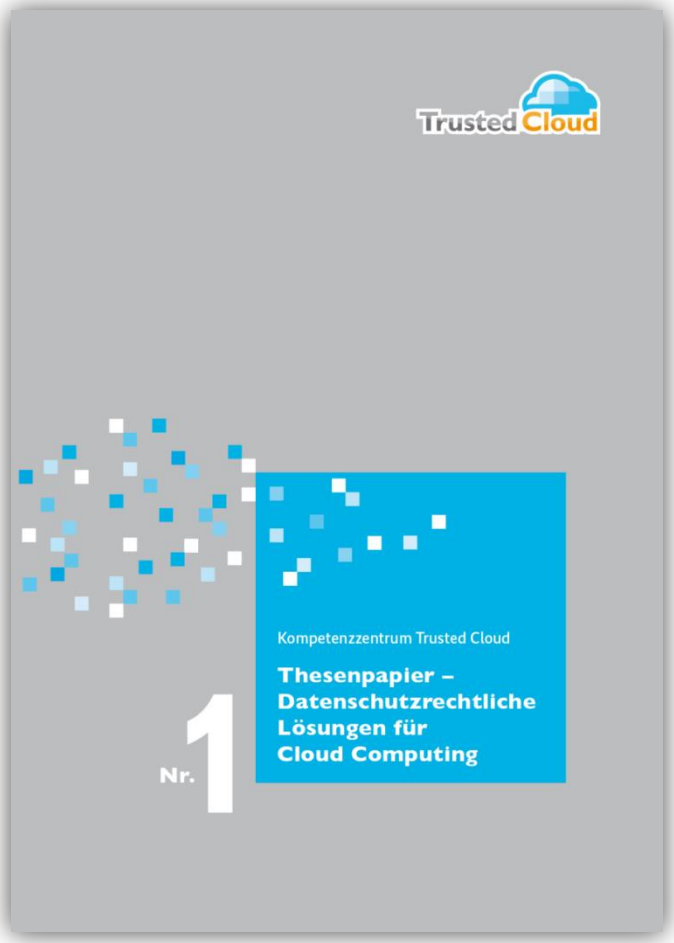
IV. Lösung: Zertifizierung

Ersetzung der eigenen Kontrolle durch ein Zertifikat

- Rechtspolitischer Vorschlag:
  Modifikation der Überwachungspflicht
  - Schutzlücken bei Verzicht auf Kontrolle
  - Haftung ist kein Ersatz für Kontrolle
  - Modifikation der Überwachungspflicht
  - Ziel: Bündelung der Kontrolle
    - durch unabhängigen Dritten
    - Dokumentation der Prüfung
    - Testat über Prüfung
    - regelmäßige Erneuerung
  - Notwendigkeit der gesetzlichen Klarstellung

IV. Lösung: Zertifizierung

Ersetzung der eigenen Kontrolle durch ein Zertifikat



IV. Lösung: Zertifizierung

Das Pilotprojekt „Datenschutzzertifizierung für Cloud-Dienste“

- Ziel:
  - Entwicklung Details der Pilot-Zertifizierung von Cloud-Diensten

- Beteiligte:
  - Datenschutzaufsichtsbehörden
  - Anbieter von Cloud-Diensten
  - Nutzer von Cloud-Diensten
  - Verbände der IT-Industrie
  - Prüfunternehmen
  - Rechtsanwälte

IV. Lösung: Zertifizierung

Das Pilotprojekt „Datenschutzzertifizierung für Cloud-Dienste“

- Phase 1 (Nov. 2013 – April 2015)
  - Grundlagen der Zertifizierung
- Phase 2 (Sept. 2015 – April 2016)
  - Durchführung der Pilot-Zertifizierung
  - Weiterentwicklung der Datenschutz-Zertifizierung

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

V. Die Reform des EU-Datenschutzrechts

- Stand der Diskussion: Vorgangs-Nr. 2012/0011 (COD)
  - Beratungen in Rat und EP seit 2012
  - Bericht Albrecht, Jan. 2013 (4.000 Änderungsvorschläge!)
  - Standpunkt des Europäischen Parlaments, März 2014
  - Vorbereitung einer Allgemeinen Ausrichtung, Ministerrat, Juni 2015
  - Entwicklung eines gemeinsamer Standpunkts von Europäischem Parlament, Rat und Kommission seit Sommer 2015 (Trilog)
- Inkrafttreten voraussichtlich: Frühjahr 2016
- Anwendbarkeit: frühestens ab 2018

V. Die Reform des EU-Datenschutzrechts

Abänderung 121, Vorschlag für eine Verordnung, Artikel 26

Auftragsdatenverarbeitung	Auftragsdatenverarbeitung
1. Der für die Verarbeitung Verantwortliche wählt für alle in seinem Auftrag durchzuführenden Verarbeitungsvorgänge einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheits-vorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.	1. Der für die Verarbeitung Verantwortliche wählt für jede in seinem Auftrag durchzuführende Verarbeitung einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheits-vorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.

V. Die Reform des EU-Datenschutzrechts

Abänderung 121, Vorschlag für eine Verordnung, Artikel 26

	3a. Die hinreichenden Garantien gemäß Absatz 1 können durch die Einhaltung von Verhaltenskodizes oder Zertifizierungsverfahren gemäß Artikel 38 oder 39 dieser Verordnung nachgewiesen werden.
4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.	4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, oder die entscheidende Partei in Bezug auf die Zwecke und Mittel der Datenverarbeitung wird, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

VI. Cloud Computing mit Auslandsbezug

Möglichkeit der Auftragsdatenverarbeitung

- Fragestellung: Kann ein ausländischer Cloud-Dienst im Rahmen einer ADV genutzt werden?

§ 3 Abs. 8 BDSG
Weitere Begriffsdefinitionen

Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

VI. Cloud Computing mit Auslandsbezug

Möglichkeit der Auftragsdatenverarbeitung

- uneingeschränkt möglich bei Cloud-Diensten aus EWR
- streitig bei Cloud-Diensten aus Drittstaaten
  - Aufsichtsbehörden: keine ADV bei Drittstaaten
  - Literatur: ADV möglich
    - Argument:
      keine Beschränkung der ADV auf EWR in Richtlinie
- Voraussetzung:
  Gewährleistung des Datenschutzes, §§ 4b, 4c BDSG

VI. Cloud Computing mit Auslandsbezug

Angemessenes Schutzniveau, § 4b BDSG

§ 4b Abs. 2 BDSG
Übermittlung personenbezogener Daten ins Ausland sowie an über- und zwischenstaatliche Stellen

[…] Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist.

- Feststellung der Angemessenheit im Einzelfall nicht praktikabel
- Feststellung des angemessenen Datenschutzniveaus durch EU-Kommission
- nur für wenige Staaten

VI. Cloud Computing mit Auslandsbezug

Andere Rechtfertigung

- Einwilligung des Betroffenen, § 4c I Nr. 1 BDSG
- Genehmigung durch Aufsichtsbehörde, § 4c II BDSG
- Standardvertragsklauseln
- Binding corporate rules
- Safe Harbor

Gliederung

I. Was ist Cloud Computing?

II. Cloud Computing und Datenschutz

III. Cloud Computing und Auftragsdatenverarbeitung

IV. Lösung: Zertifizierung

V. Die Reform des EU-Datenschutzrechts

VI. Cloud Computing mit Auslandsbezug

VII. Safe Harbor

VII. Safe Harbor

- Die Safe Harbor-Grundsätze
  - Hrsg. durch US Department of Commerce, 2000
  - Beratungen in Rat und EP seit 2012
  - Gegenstand: sieben Datenschutzgrundsätze
  - „Selbst-Zertifizierung“:
    Registrierung von Unternehmen in Liste aufgrund jährlicher Erklärung, die Grundsätze zu befolgen

VII. Safe Harbor

- Entscheidung der EU-Kommission 2000/520, 26.7.2000
  - Entscheidung nach Art 25. Abs. 6 DS-RL
  - Inhalt:
    Angemessenes Datenschutz-Niveau i.S.v. Art. 25 II DS-RL bei Selbstverpflichtung nach Safe Harbor
  - Wirkung:
    Übermittlung von Daten an registrierte Stellen in USA zulässig wie an Stellen innerhalb des EWR

VII. Safe Harbor

- Urteil des EuGH, 6.10.2015, C362/14
  - Vorabentscheidung im Fall Facebook (Vorlage High Court Irland)
  - Tenor: **„Die Entscheidung 2000/520 ist ungültig.“**
  - Begründung:
    - EU-Kommission hat Bestehen eines angemessenen Datenschutzes in USA nicht festgestellt
    - Kein angemessener Datenschutz in USA
    - Selbstzertifizierung genügt nur bei Existenz wirksamer Überwachungs- und Kontrollmechanismen

VII. Safe Harbor

- Grundlagen für Datentransfer in die USA
  - Nicht mehr: Safe Harbor / Kommissionsentscheidung 2000
  - Künftig ggf. „Safe Harbor II“???
  - ULD Kiel, Positionspapier
    - derzeit keine taugliche Grundlage
  - Literatur
    - alle anderen Grundlagen, insb. Standardvertragsklauseln, binding corporate rules etc.

Vielen Dank für Ihre Aufmerksamkeit!

Prof. Dr. Georg Borges

georg.borges@uni-saarland.de

www.georgborges.de

www.rechtsinformatik.saarland