

DATENSCHUTZ UND DATENSICHERHEIT

HARDER
RECHTSANWÄLTE

BÜSING
MÜFFELMANN
& THEYE

BREMEN
FRANKFURT AM MAIN
BERLIN
MÜNCHEN



Bei Datenportabilität und Single Sign-On im Multi-Cloud-Umfeld



BMT
München

Bernd H. Harder
Rechtsanwalt
Dr. Christian Weitzel
Fachanwalt für Informationstechnologierecht

www.bmt.eu



BMT



Ihre Referenten



Bernd H. Harder

Rechtsanwalt

Tel. (+49) 0 89 28 70 07-0
Fax (+49) 0 89 28 70 07-29
Mobil (+49) 0 171 8817000
E-Mail harder@bmt.eu

VITA

- Jurastudium und Referendariat in Heidelberg
- 1978–1981 · Syndikus im Unilever-Konzern/Langnese-Iglo, Hamburg
 - 1981–1991 · Syndikus, Vertriebsmanager und Leiter Unternehmensverbindungen bei Digital Equipment (DEC), München
 - 1991–1997 · European IT/S-Practice Manager bei McKinsey & Co., Düsseldorf
 - 1997–2002 · Partner bei Graefe & Partner Rechtsanwälte, München
 - 2002–2008 · Gründer und Partner HARDER Rechtsanwälte, München
 - seit 2008 · Partner bei Büsing, Müffelmann & Theye, München



Ihre Referenten



DR. CHRISTIAN WEITZEL

Fachanwalt für Informationstechnologierecht

Tel. (+49) 0 89 28 70 07-0
Fax (+49) 0 89 28 70 07-29
Mobil (+49) 0 170 4752492
E-Mail weitzel@bmt.eu

VITA

Jurastudium, Promotion (1998) und Referendariat in Münster
Informatikstudium in Hagen
1997–1998 · Rechtsanwalt in Frankfurt
1998–2009 · Diverse Positionen bei Giesecke & Devrient in München
seit 2006 · Lehrbeauftragter der TU Wien (IT-Strategie, Risikomanagement)
seit 2009 · Partner bei Büsing, Müffelmann & Theye



AGENDA



1

Einstieg: Datenschutz oder Datensicherheit?

2

Daten tragen durch die Cloud

3

Gängige Tipps

4

Terra Incognita

5

Single Sign-On

6

Ausblick

JA WAS NUN GENAU?

- **Datenschutz** hatten wir schon lange ...
 - So viel neues enthält die DS-GVO nicht.
- **Datensicherheit** wird plötzlich gehypt.
 - Gab es schon „durch die Hintertür“:
TOMs nach § 9 BDSG (alt)



SCHAUEN WIR GENAU HIN:



§ 9 BDSG (alt)

Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, **um die Ausführung der Vorschriften dieses Gesetzes**, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.

SCHAUEN WIR GENAU HIN:



§ 9 BDSG (alt)

Technische und organisatorische Maßnahmen

Öffentliche und im Auftrag der Verantwortlichen selbst oder im Auftrag der Verantwortlichen durch Dritte im Auftrag der Verantwortlichen oder nur für die Verantwortlichen durch Dritte ergriffenen Maßnahmen

Ausführung dieser Maßnahmen, insbesondere die Erfüllung der in den Absätzen 1 bis 4 genannten Anforderungen zu gewährleisten.

Kein einziges Wort zu Datensicherheit

EHEMALS: ECHTE DUALITÄT



- Gipfelte manchmal in der Vorstellung:
 - Datensicherheit ist außergesetzlich geregelt – wenn überhaupt!

NEU: KLARE GESETZLICHE VERANKERUNG



§ 64 BDSG (neu)

Anforderungen an die **Sicherheit der Datenverarbeitung**

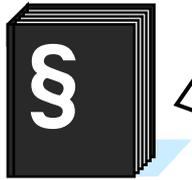
- (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die **erforderlichen technischen und organisatorischen Maßnahmen** zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten (...)

Art. 5 DS-GVO

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

- f) einer Weise verarbeitet werden, die eine angemessene **Sicherheit der personenbezogenen Daten** gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung **durch geeignete technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“);





Art. 32 DS-GVO
Sicherheit der Verarbeitung

- (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (...)

NEU: KLARE GESETZLICHE VERANKERUNG



Weitere Normen in der DS-GVO
spezifisch zur **Sicherheit** der Verarbeitung

Art. 24 DS-GVO: Verantwortung des für die Verarbeitung
Verantwortlichen

Art. 25 DS-GVO Datenschutz durch Technikgestaltung und
durch datenschutzfreundliche Voreinstellungen

Art. 36 DS-GVO Vorherige Konsultationen

WICHTIGE ERKENNTNIS NR. 1

- **Datenschutz** und **Datensicherheit** sind jetzt eins.



WICHTIGE ERKENNTNIS NR. 2

- Datenschutz und Datensicherheit sind jetzt eins.
- Datenschutz **durch** Datensicherheit ist die Prämisse.



ODER, ANDERS GESAGT:

- Rechtskonformes Verhalten („**Compliance**“) durch **sichere Technik**-Gestaltung.





AGENDA



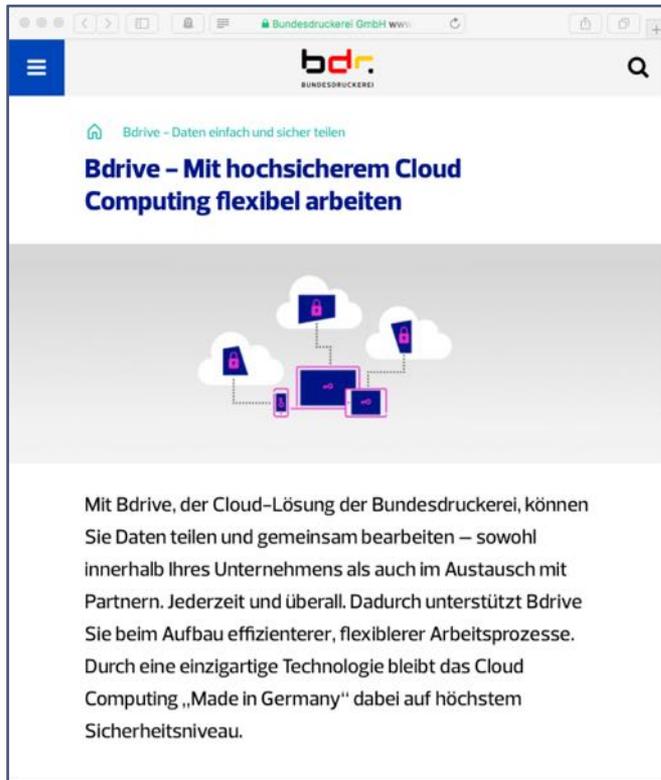
- 1 Einstieg: Datenschutz oder Datensicherheit?
- 2 Daten tragen durch die Cloud**
- 3 Gängige Tipps
- 4 Terra Incognita
- 5 Single Sign-On
- 6 Ausblick

DER TRAUM ...

- Freie Portabilität aller Daten
 - Quer durchs Internet
 - Von einer Cloud in die andere
 - Von einem Provider zum anderen



... WIRD ENDLICH WAHR?



The screenshot shows a web browser window with the URL 'Bundesdruckerei GmbH www...'. The page header features the 'bdr' logo and a search icon. Below the header, there is a navigation bar with a home icon and the text 'Bdrive - Daten einfach und sicher teilen'. The main heading reads 'Bdrive - Mit hochochsigem Cloud Computing flexibel arbeiten'. A central graphic depicts a cloud with various devices (laptop, tablet, smartphone) connected to it. Below the graphic, a paragraph of text describes the benefits of Bdrive.

Bdrive - Mit hochochsigem Cloud Computing flexibel arbeiten

Mit Bdrive, der Cloud-Lösung der Bundesdruckerei, können Sie Daten teilen und gemeinsam bearbeiten – sowohl innerhalb Ihres Unternehmens als auch im Austausch mit Partnern. Jederzeit und überall. Dadurch unterstützt Bdrive Sie beim Aufbau effizienterer, flexiblerer Arbeitsprozesse. Durch eine einzigartige Technologie bleibt das Cloud Computing „Made in Germany“ dabei auf höchstem Sicherheitsniveau.

... WIRD ENDLICH WAHR?

Bdrive - Mit Computing

HOME » CLOUD COMPUTING » **ENDLICH SICHERES CLOUD COMPUTING: OFFICE 365 VON DER TELEKOM**

ENDLICH SICHERES CLOUD COMPUTING: OFFICE 365 VON DER TELEKOM

Dieser Artikel wurde veröffentlicht von [Jens Hagel](#).

Cloud-Computing gestattet es, Dokumente gemeinsam mit Kollegen online zu bearbeiten und auf dem Server abzuspeichern. In Deutschland bereitete es Unternehmen bislang oftmals Kopfzerbrechen, sich für die innovative Cloudnutzung zu entscheiden. Der Grund dafür ist, dass die Cloud-Office-Dienstleistungen von amerikanischen Unternehmen wie Google, Apple und Microsoft zur Verfügung gestellt werden. Diese Konzerne sind von Seiten des Staates dazu verpflichtet, mit der NSA und mit zahlreichen weiteren Behörden zusammenzuarbeiten.

CLOUD storage

... WIRD ENDLICH WAHR?

Bdrive - Mit Computing

hagel services

HOME » CLOUD COMPUTING » TELEKOM

ENDLICH SICHERES

Dieser Artikel wurde veröffentlicht

Cloud-Computing gestattet es, Dokumente gemeinsam mit Kollegen online zu bearbeiten und auf dem Server abzuspeichern. In Deutschland ist es Unternehmen bislang oftmals schwer gefallen, sich für die intensive Cloudnutzung zu entscheiden. Grund dafür ist, dass die Cloud-Office-Dienstleistungen von amerikanischen Unternehmen wie Google, Apple und Microsoft zur Verfügung gestellt werden. Diese Konzerne sind von Seiten des Bundesstaates dazu verpflichtet, mit den Unternehmen und mit zahlreichen weiteren Behörden zusammenzuarbeiten.

Cloud Computing Insider

Sie befinden sich hier: [Plattformen](#)

CeBIT 2014: Canopy-Portfolio soll offensiv vermarktet werden
Atos zeigt sicheres Cloud Computing

10.02.14 | Autor / Redakteur: Dirk Strocke / Florian Karistetter

What can the cloud really do for businesses?

Neben vielfältigen Cloud-Lösungen präsentiert Atos das mit dem Enterprise Social Network blueKiwi umgesetzte "zero email"-Projekt. (Bild: Atos/Canopy)

Sichere Cloud-Lösungen für Unternehmen will Atos auf der CeBIT präsentieren. Angekündigt sind Data Analytics as a Service, das Produktportfolio der Tochter Canopy sowie das Enterprise Social Network blueKiwi.

... WIRD ENDLICH WAHR?

Bdrive - Mit Cloud Computing...

hagel services

HOME » CLOUD COMPUTING » TELEKOM

ENDLICH SICHERES CLOUD COMPUTING

Dieser Artikel wurde veröffentlicht...

Cloud-Computing gestattet es, Dokumente gemeinsam mit Kollegen online zu bearbeiten und auf dem Cloud-Speicher abzuspeichern. In Deutschland ist es Unternehmen bislang oftmals ein Kopfzerbrechen, sich für die in der Cloudnutzung zu entscheiden. Dafür ist, dass die Cloud-Office-Dienstleistungen von amerikanischen Unternehmen wie Google, Apple und Microsoft zur Verfügung gestellt werden. Diese Konzerne sind von Seiten des Staates dazu verpflichtet, mit den Kunden und mit zahlreichen weiteren Betreibern zusammenzuarbeiten.

CeBIT 2014: Canopy-Portfolio soll offensiv vermarktet werden - Atos zeigt sicheres Cloud Computing

10.02.14 | Autor / Redakteur: Dirk Strocke / Florian Karlstetter

CloudComputing Insider

Sie befinden sich hier: Plattformen

Atos zeigt sicheres Cloud Computing

Neben vielfältigen Cloud-Lösungen präsentiert Atos das mit dem "email"-Projekt. (Bild: Atos/Canopy)

Sichere Cloud-Lösungen für Unternehmen präsentieren. Angekündigt sind Data und Produktportfolio der Tochter Canopy blueKiwi.

PR&D

Suchergebnisse | PR&D Kommunikations... | Sicheres Cloud Computing ist kein Wo...

PR&D - PUBLIC RELATIONS FÜR FORSCHUNG & BILDUNG

TÄTIGKEITSBEREICH - LEISTUNGSSPEKTRUM - AGENTUR - KUNDEN - **KUNDEN-NEWS**

KUNDEN-NEWS

WISSENSCHAFT
15. September 2014

FWF
Der Wissenschaftsfonds.
← Zurück zur Übersicht

IT Security

Quality Management

IT Management

Model Engineering

Business Processes & Workflows

Sicheres Cloud Computing ist kein Wolkenkuckucksheim

Integration von digitalem Fachwissen und Automatisierung von Risiko-Analysen kann Testverfahren für Software deutlich verbessern und Cloud Computing sicherer machen. Das zeigen neueste Ergebnisse eines Projekts des Wissenschaftsfonds FWF zur Qualitätssicherung sicherheitskritischer Systeme, die soeben veröffentlicht wurden. Die Ergebnisse bilden eine Grundlage für sogenannte nicht-funktionale Sicherheitstests. Diese sollen Schwachstellen von Software identifizieren, die sich nicht aus dem unmittelbaren Programmablauf ergeben – und spielen für Cloud Computing eine immer wichtigere Rolle. Mit den nun entwickelten Grundlagen können solche Tests weiter automatisiert und nutzerfreundlicher gemacht werden.

... WIRD ENDLICH WAHR?

The collage features several overlapping browser windows:

- hagel services**: A window showing a navigation menu with 'HOME' and 'CLOUD COMPUTING TELEKOM'.
- CeBIT 2014: Canopy-Portfolio soll offensiv vermarktet werden. Atos zeigt sicheres Cloud Computing**: A news article snippet dated 10.02.14, mentioning 'Autor / Redakteur: Dirk Strocke / Florian Karlistetter'.
- PR&D - PUBLIC RELATIONS FÜR FORSCHUNG & BILDUNG**: A window showing a navigation menu with 'TÄTIGKEITSBEREICH', 'LEISTUNGSSPEKTRUM', 'AGENTUR', 'KUNDEN', and 'KUNDEN-NEWS'.
- WISSENSCHAFT 15. September 2014**: A window featuring a diagram and the text 'Sicheres Cloud Computing ist kein Wolkenkuckucksheim'.

The magnifying glass is focused on a diagram with the following elements:

- IT Security**
- Quality Management**
- Business Processes & Workflow**
- Model Engineering**
- Management**

The diagram shows a central globe with arrows indicating a cycle between these components.

TRÄUME SIND SCHÄUME

- Ganz ehrlich: Es geht gar nicht bloß um Daten
 - Ganze VMs, Container (Docker) oder Server (Box)
- Ständige Bewegung lässt Kosten für Netz explodieren
- Easy Cloud Access lässt Schatten-IT aufblühen



AGENDA



- 1 Einstieg: Datenschutz oder Datensicherheit?
- 2 Daten tragen durch die Cloud
- 3 Gängige Tipps**
- 4 Terra Incognita
- 5 Single Sign-On
- 6 Ausblick

WAS DIE TECHNIKER EMPFEHLEN

1. Verschlüsseln der Daten

- Braucht unterschiedliche Schlüssel für jede Plattform
- Verschieben der Daten zwischen Plattformen wird schwerer
- Hilft bei unzulässiger Lokation der Plattform auch nicht weiter



Jim O'Reilly

2. Erasure Coding

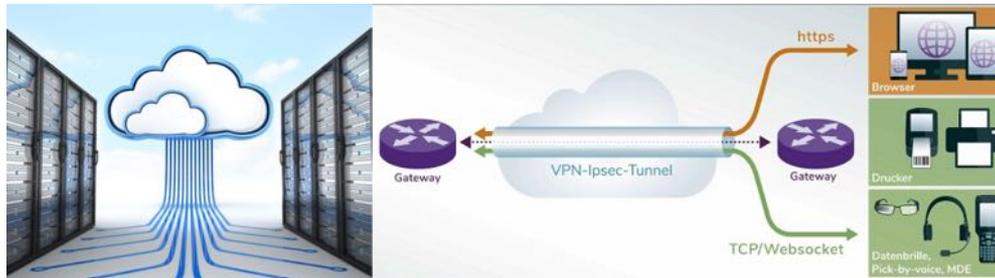
- Aufteilen der Daten in viele kleine Fragmente, verteilt über viele Plattformen
- Rechenintensiv und praktisch von kaum einer Applikation unterstützt

3. Datenkompression

- Komprimierte Daten sind per se kodiert
- Nur: Welche Applikation in der Cloud kann mit den Daten arbeiten?

JETZT NOCH MAL VERSCHLÜSSELUNG

- Das Stichwort gibt es doch auch in der DS-GVO?
 - Art. 5 Abs. 1 lit. e) und f) sind letztlich nur mit Anonymisierung/Verschlüsselung einzuhalten
- Was heißt das jetzt für die Cloud?
 - Überall gibt es:
Tunnel-Verschlüsselung für den Weg in die Cloud



Die IT-Security Messe und Kongress
The IT Security Expo and Congress

JETZT NOCH MAL VERSCHLÜSSELUNG

- Das Stichwort gibt es doch auch in der DS-GVO?
 - Art. 5 Abs. 1 lit. e) und f) sind letztlich nur mit Anonymisierung/Verschlüsselung einzuhalten
- Nur was keiner bietet:
 - Verarbeitung verschlüsselter Daten in der Cloud



UND WAS EMPFIEHLT IHR JURIST ...

- ... zum Umfang der Verschlüsselung in der Cloud?
- Haben Sie dazu überhaupt schon einmal mit ihm gesprochen?
- Oder dem Datenschutzbeauftragten?



AGENDA



- 1 Einstieg: Datenschutz oder Datensicherheit?
- 2 Daten tragen durch die Cloud
- 3 Gängige Tipps
- 4 Terra Incognita**
- 5 Single Sign-On
- 6 Ausblick

„Law always lags behind technology.“

Michael I. Meyerson

Professor of Law, University of Baltimore

Die spannende Frage:

- Gilt das auch für die „brandneue“ DS-GVO?



VERWIRRUNG IN DER BUZZ WORD CLOUD

1. Private Cloud

- Rechtlich unproblematisch – nur immer seltener
- Und nach Ansicht vieler Kunden und Anbieter obsolet



2. Community Cloud

- Mischung von private und public cloud
- z.B. Microsoft Office 365 als SaaS



3. Public Cloud

- z.B. Amazon Web Services, Microsoft Azure



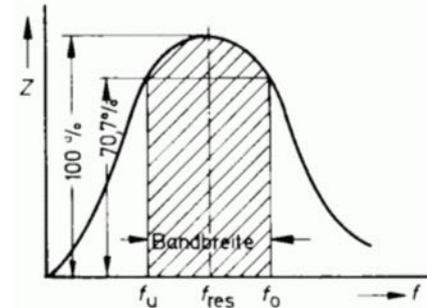
4. Hybrid Cloud / Multi Cloud

- Mischung der vorgenannten mit Last-Verschiebung je nach Anforderung, Kosten oder Praktikabilität



WO ES SCHON SCHWIERIG WIRD:

1. Wer ist Auftraggeber („Controller“), wer Verarbeiter („Processor“) beim Cloud Computing?
 - Wer trägt die Verantwortung bei Verstößen?
 - Welche Pflichten muss der Partner selbst einhalten?
- In Deutschland weitgehend einheitlich beurteilt
- Ganz anders international:
 - Cloud Service Provider ist Processor
 - Cloud Service Provider ist Controller
 - Cloud Service ist gemeinsame Verantwortung
 - Nichts von alledem, neutraler Vermittler



WO ES SCHON SCHWIERIG WIRD:

1. Wer ist Auftraggeber („Controller“), wer Verarbeiter („Processor“) beim Cloud Computing?
 - Wer trägt die Verantwortung bei Verstößen?
 - Welche Pflichten muss der Partner selbst einhalten?

2. Ab wann verwischen die Grenzen?
 - Mit der Folge gemeinsamer Verantwortung („Joint Controllershhip“)

WO ES SCHON SCHWIERIG WIRD:

1. Wer ist Auftraggeber („Controller“), wer Verarbeiter („Processor“) beim Cloud Computing?
 - Wer trägt die Verantwortung bei Verstößen?
 - Welche Pflichten muss der Partner selbst einhalten?

2. Ab wann verwischen die Grenzen?
 - Mit der Folge gemeinsamer Verantwortung („Joint Controllershhip“)
 - bei IaaS?
 - bei PaaS?
 - bei SaaS?
 - mit voller Gestaltungsfreiheit?
 - mit vielen Service Levels?

WO ES SCHON SCHWIERIG WIRD:

1. Wer ist Auftraggeber („Controller“), wer Verarbeiter („Processor“) beim Cloud Computing?
 - Wer trägt die Verantwortung bei Verstößen?
 - Welche Pflichten muss der Partner selbst einhalten?
2. Ab wann verwischen die Grenzen?
 - Mit der Folge gemeinsamer Verantwortung („Joint Contollership“)
3. Betroffenenrechte
 - Nachricht über Ort der Datenverarbeitung?
4. Audit-Recht und Kontrollpflicht
 - Vor-Ort-Besuch bei welchem Amazon-Rechenzentrum?
 - Persönliche Kontrolle unbekannter Infrastrukturen?

LÄSST SICH DAS NICHT VEREINHEITLICHEN?

Schauen wir auf die TOMs:

Anlage zu § 9 Satz 1 BDSG (alt)

- | | |
|----|-------------------------|
| 1. | Zutrittskontrolle |
| 2. | Zugangskontrolle |
| 3. | Zugriffskontrolle |
| 4. | Weitergabekontrolle |
| 5. | Eingabekontrolle |
| 6. | Auftragskontrolle |
| 7. | Verfügbarkeitskontrolle |

LÄSST SICH DAS NICHT VEREINHEITLICHEN?

Schauen wir auf die TOMs:

Anlage zu § 9 Satz 1 BDSG (alt)		§ 64 Abs. 3 BDSG (neu)	
1.	Zutrittskontrolle	1.	Zugangskontrolle
2.	Zugangskontrolle	2.	Datenträgerkontrolle
		3.	Speicherkontrolle
		4.	Benutzerkontrolle
3.	Zugriffskontrolle	5.	Zugriffskontrolle
4.	Weitergabekontrolle	6.	Übertragungskontrolle
5.	Eingabekontrolle	7.	Eingabekontrolle
		8.	Transportkontrolle
		9.	Wiederherstellbarkeit
		10.	Zuverlässigkeit
		11.	Datenintegrität
6.	Auftragskontrolle	12.	Auftragskontrolle
7.	Verfügbarkeitskontrolle	13.	Verfügbarkeitskontrolle
		14.	Trennbarkeit

LÄSST SICH DAS NICHT VEREINHEITLICHEN?

One fits all – passt nur selten!

§ 64 Abs. 3 BDSG (neu)		Office 365 SaaS	Docker PaaS	Box IaaS
1.	Zugangskontrolle	X	~	~
2.	Datenträgerkontrolle	X	X	X
3.	Speicherkontrolle	X	~	
4.	Benutzerkontrolle	~	~	
5.	Zugriffskontrolle	X	~	
6.	Übertragungskontrolle	X		
7.	Eingabekontrolle	~		
8.	Transportkontrolle	X		
9.	Wiederherstellbarkeit	X	X	X
10.	Zuverlässigkeit	X	~	~
11.	Datenintegrität	X	X	
12.	Auftragskontrolle	X		
13.	Verfügbarkeitskontrolle	X	X	X
14.	Trennbarkeit	X	X	X



Compliance: wer muss welche Pflichten erfüllen?

- Vorherige schriftliche Genehmigung von Unterverarbeitern, Art. 28 Abs. 2 DS-GVO
 - Ist der Wettbewerber in der Multi-Cloud ein Unterverarbeiter?
 - Kann/sollte der Kunde es so gestalten?
 - Will ein Cloud-Provider der Multi Vendor Manager sein?
 - Ist das sinnvoll?
- Auferlegung derselben Pflichten an Unterverarbeiter, Art. 28 Abs. 4 DS-GVO
 - Haftung des Haupt-Auftragverarbeiters für Verstöße des Unterverarbeiters!
- Datenschutz-Folgenabschätzung, Art. 35 Abs. 1 DS-GVO
 - Wie vorab bei durch die Multi-Cloud wandernden Daten?
- Meldung von Datenschutzverletzungen, Art. 33 DS-GVO
 - Wer muss die 72-Stunden-Frist einhalten?

Wer haftet, wer kann Verantwortung von sich weisen?

- Bei mehreren Auftragsverarbeitern oder gemeinsamer Verantwortung:



Art. 82 DS-GVO Haftung und Recht auf Schadensersatz

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet **jeder Verantwortliche** oder **jeder Auftragsverarbeiter für den gesamten Schaden**, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

WIESO IST DAS SO WICHTIG?

- Bei mehreren Auftragsverarbeitern oder gemeinsamen Verantwortungen

Geimeinsame Haftung mit anderen Providern – welcher Provider will das denn?

DS-GVO

Art. 82 Abs. 1 S. 1 DSGVO – Schadensersatz

Wenn ein Verantwortlicher oder ein Auftragsverarbeiter an derselben Stelle tätig ist und die Verarbeitung der personenbezogenen Daten ausschließlich im Namen des Verantwortlichen erfolgt, so haftet **jeder** Verantwortliche oder **jeder Auftragsverarbeiter** für den Schaden, den die betroffene Person erleidet.

§

der Verantwortliche oder der Auftragsverarbeiter, der den Schaden verursacht hat, ist für die entstandenen Schäden verantwortlich.

WIESO IST DAS SO WICHTIG?

- Bei mehreren Auftragsverarbeitern oder gemeinsamen Verantwortlichkeiten

In der Multi-Cloud nachweisen, dass mehrere Provider verantwortlich sind –
welcher Kunde will das denn?

Datenschutz

mehr als ein Verantwortlicher an derselben Verarbeitung gemäß den Verantwortlich, so haftet **jeder Auftragsverarbeiter**, damit ein wirksamer offene Person

WAS PAUSCHALER RAT NICHT SAGEN KANN

1. Rechtswirksame Auftragsverarbeitung

- Weisungen?
- Kontrolle?
- Zuordnung Verantwortung?

2. Besonders schutzwürdige Daten

- Betriebsarzt: Gesundheitsdaten
- HR: Religion, sexuelle Besonderheiten
- Finanzdaten: § 25a KWG

3. Betroffenenrechte

- Nachricht über Ort der Datenverarbeitung?
- Sonstige Informationspflichten?

Ohne Details zum Sachverhalt
(=Karte und Navigation)





AGENDA



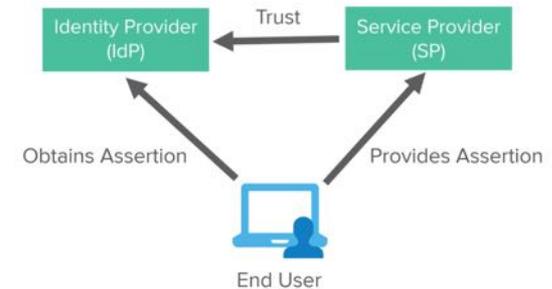
- 1 Einstieg: Datenschutz oder Datensicherheit?
- 2 Daten tragen durch die Cloud
- 3 Gängige Tipps
- 4 Terra Incognita
- 5 Single Sign-On**
- 6 Ausblick

SSO: VON KOMPLIZIERT ZU HOCH-KOMPLEX

- **Auslöser: Identity Access Management (IAM)**
 - Typischer Unternehmensbedarf:
 - SAP/Salesforce, Box, Slack und Office 365
 - Und 150 verschiedene weitere Anwendungen ...
- **Bei on-premise-Lösung unter einer Kontrolle**
 - Nur ein technisches Problem

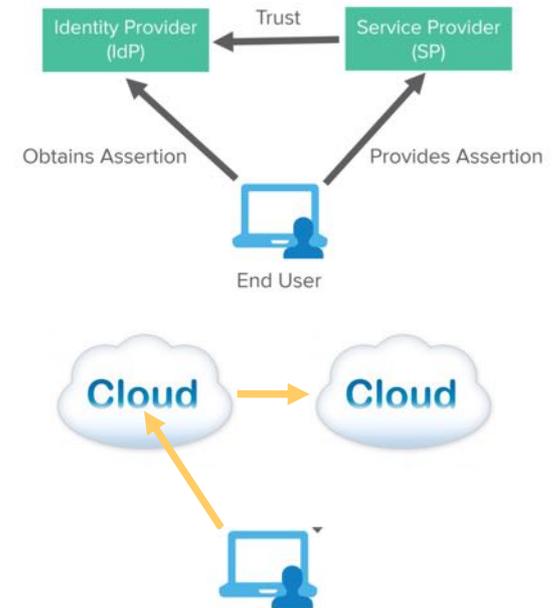
SSO: VON KOMPLIZIERT ZU HOCH-KOMPLEX

- Auslöser: Identity Access Management (IAM)
 - Typischer Unternehmensbedarf:
 - SAP/Salesforce, Box, Slack und Office 365
 - Und 150 verschiedene weitere Anwendungen ...
- Bei on-premise-Lösung unter einer Kontrolle
 - Nur ein technisches Problem
- Mit der Cloud wird alles easy? Leider nicht:
 - Modebegriff „Federated Identity“
 - Braucht Externe Cloud Identity Provider (IdP)



SSO: VON KOMPLIZIERT ZU HOCH-KOMPLEX

- **Auslöser: Identity Access Management (IAM)**
 - Typischer Unternehmensbedarf:
 - SAP/Salesforce, Box, Slack und Office 365
 - Und 150 verschiedene weitere Anwendungen ...
- Bei on-premise-Lösung unter einer Kontrolle
 - Nur ein technisches Problem
- Mit der Cloud wird alles easy? Leider nicht:
 - Modebegriff „Federated Identity“
 - Braucht Externe Cloud Identity Provider (IdP)



- SSO wird zum Single Point of Failure



Pflicht zur Bereitstellung der nötigen Verfügbarkeit nach Art. 32 Abs. 1 lit. b) DS-GVO

- Welche Daten dürfen in der Zugriffsmöglichkeit eines externen IdP stehen?



Pflicht zum Schutz vor unrechtmäßiger Verarbeitung (Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f) DS-GVO

- Welche Rolle hat der IdP eigentlich – Controller oder Processor?



Und was regelt dazu die EIDAS-Verordnung (EU) Nr. 910/2014?

UND JETZT DIE PROBLEME

- SSO wird zum Single Point of Failure



Pflicht zur Bereitstellung von Informationen zur Verfügbarkeit nach Art. 52 DSGVO

- Welche Pflichten haben Verantwortliche gegenüber externen Dienstleistern?



Pflicht zur Bereitstellung von Informationen zur Verfügbarkeit (Interaktion mit Art. 52 DSGVO, Art. 1 lit. f) DS-GVO

- Welche Rolle spielen Verantwortliche bei der Auswahl von Cloud-Provider oder Processor?



Und was ist die Rolle des Verantwortlichen bei der Auswahl von Cloud-Provider oder Processor (EU) Nr. 910/2014?

Alles Fragen,
deren Antwort von
der Ausgestaltung
im jeweiligen
Einzelfall
abhängt.



AGENDA



- 1 Einstieg: Weshalb eine Schulung zu OSS?
- 2 OSS: Was ist das überhaupt?
- 3 OSS-Lizenzen und ihre Unterschiede
- 4 OSS im kommerziellen Einsatz
- 5 Single Sign-On
- 6 Ausblick**

- Keine einfache Sache
 - DS-GVO-Compliance im Multi-Cloud-Umfeld
- Jedenfalls dann, wenn
 - Man sich nicht um viel kümmern will (frei wabernde Daten in der Cloud)
 - Die Lokationen einem egal sind
 - Die Daten nicht aufgeteilt sind (nach Schutzwürdigkeit)
 - Alles nur billig sein soll

1. Modalitäten des Einzelfalls dominieren die Lösung.
 - Das macht „out-of-the-box“-Lösungen schwer.
2. Den Standard kann es so schnell nicht geben.
 - Weil Anforderungen und Datenkategorien der Kunden so unterschiedlich sind.
3. Datenschutz ist kein Geschäftsverhinderer.
 - Schwierige, differenzierte Anforderungen lassen sich nicht mit einfachen Lösungen erfüllen.
4. Techniker und Juristen müssen enger zusammenrücken.
 - Um die komplexen, eng verschränkten Fragen zu klären.
5. Juristen müssen viel mehr von Technik lernen und verstehen.
 - Um die zu lösenden Probleme zu sehen und einstufen zu können.

HANDLUNGSOPTIONEN

1. Weitermachen wie bisher

- Augen zu und durch
- Und hoffen, dass es nicht so bald kracht ...



2. Sorgfältig hinschauen und Datensicherheit erstmals richtig handhaben.



UND JETZT: NOCH FRAGEN?





Vielen Dank.
Kontaktieren sie uns!



STANDORT
BERLIN

Kurfürstendamm 190/192
10707 Berlin



STANDORT
BREMEN

Marktstraße 3, Börsenhof C
28195 Bremen



STANDORT
FRANKFURT

Taunusanlage 18
60325 Frankfurt



STANDORT
MÜNCHEN

Maximilianstrasse 38
80539 München