

Public Cloud für die öffentliche Hand

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

Ihr Referent

Haupttätigkeit:

Stabsstelle IT-Recht
der bayerischen staatlichen Universitäten und Hochschulen

Hintergrund:

- Volljurist
Studium Ludwig-Maximilians-Universität
Referendariat OLG München, Wahlstation bei Eversheds UK
- Rechtsinformatikzertifikat an der Ludwig-Maximilians-Universität
- Zertifizierter Informationssicherheitsbeauftragter (OTH Regensburg)
- Microsoft Licensing Professional
- Twitter privat: [@JoNehlsen](#)

Nachrichten aus Ferne

Trump vs. Bezos: Militär-Cloud JEDI aufgeschoben

Der Auftrag für die US-Militär-Cloud "JEDI" verzögert sich, nachdem das Weiße Haus die Vergabe überprüfen lässt. Im Rennen waren Microsoft und Amazon.

Bank-Hack nicht hilfreich

Der Bank-Hack bei Capital One mit über 100 Millionen Betroffenen bedeutet zusätzlichen Gegenwind für Amazon. Die gehackten Systeme sind bei AWS gehostet. Zwar haben sowohl Amazon als auch Capital One betont, die entscheidende Fehlkonfiguration der Firewall sei im Bereich Capital Ones gelegen und kein Fehler der AWS-Cloud. Dennoch hat ein Ausschuss des US-Unterhauses bei beiden Unternehmen Informationen zu dem Vorfall angefordert und dabei explizit den JEDI-Auftrag erwähnt.

<https://www.heise.de/newsticker/meldung/Trump-vs-Bezos-Militaer-Cloud-JEDI-aufgeschoben-4486982.html> 02.08.2019



Nachrichten über Bodycams

Medienbericht: Bundespolizei speichert Bilder bei Amazon - Kritik vom Datenschutzbeauftragten

SPIEGEL ONLINE - Panorama - 25.03.2019

Die Bundespolizei speichert Bodycam-Daten bei Amazon. Der Bundesdatenschutzbeauftragte hält das für problematisch - und fordert den Wechsel zu einem deutschen Cloud-Anbieter. **mehr...**

<https://www.spiegel.de/panorama/justiz/amazon-datenschutzbeauftragter-kritisiert-speicherung-von-polizeibildern-a-1259475.html>



"St. Paddy's Day in North Charleston - 2016" by [North Charleston](#) is licensed under [CC BY-SA 2.0](#)

Nachrichten über die Deutsche Cloud

Fehlende Nachfrage: Microsoft stellt „Deutsche Cloud“ ein

SPIEGEL ONLINE - Netzwelt - 03.09.2018

Mit seinem deutschen Cloud-Angebot traf Microsoft vor drei Jahren den Nerv der Zeit: Edward Snowden und die NSA-Affäre hatten viele Nutzer sensibilisiert. Nun wird der Vertrieb eingestellt - aus mangelndem Interesse. **mehr...**

<https://www.spiegel.de/netzwelt/web/deutsche-cloud-microsoft-stellt-vertrieb-seines-datendienstes-ein-a-1226307.html>

In geheimen Rechenzentren: Microsoft führt neue „Deutsche Cloud“ ein

SPIEGEL ONLINE - Netzwelt - 28.08.2019

Vor einem Jahr stellte Microsoft seine deutsche Cloud ein. Jetzt startet der Konzern einen zweiten Versuch: Kundendaten sollen künftig zwar in Deutschland gespeichert werden, aber an weltweite Netze angebunden sein. **mehr...**

<https://www.spiegel.de/netzwelt/web/microsoft-fuehrt-neue-deutsche-cloud-ein-a-1283985.html>



Public Cloud

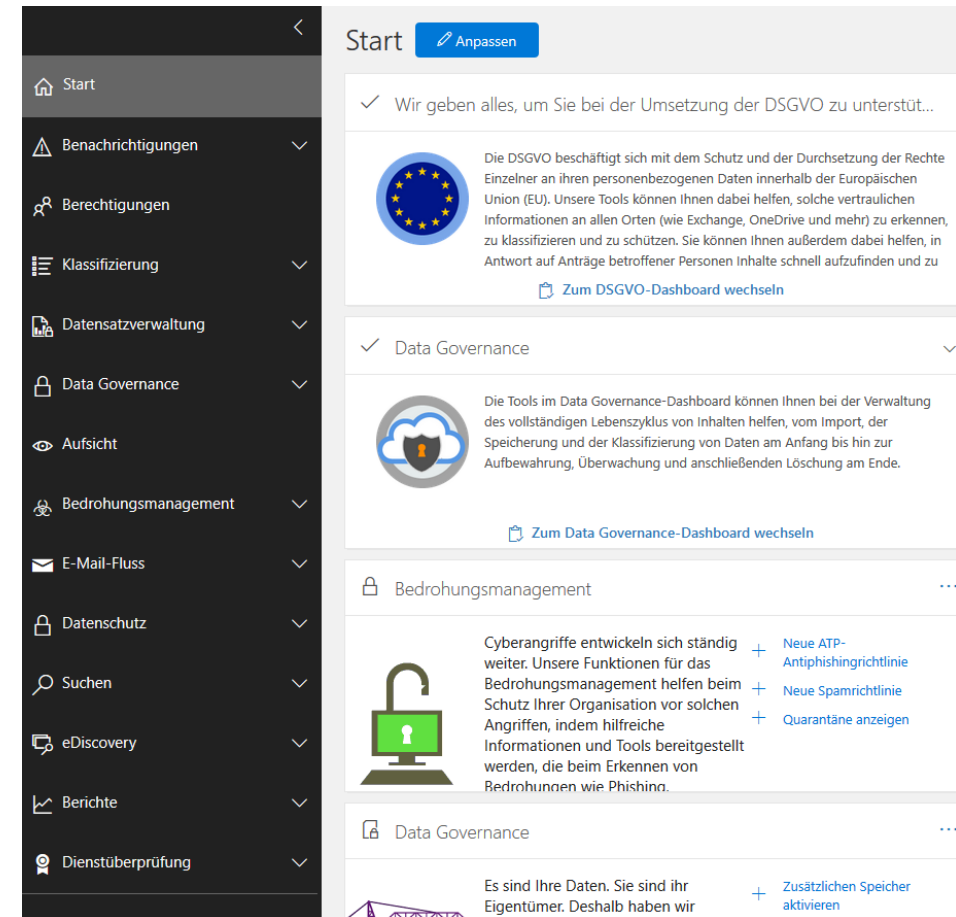
- ~~Hochschul-Rechenzentren~~
- ~~Föderierte DFN Clouddienste~~
- Amazon, Google, Microsoft, Oracle, IBM, Alibaba, ...
- Fabasoft, SAP, Cancom, ...
- Software as Service
 - Adobe Document Cloud und Creative Cloud
 - Dropbox Business
 - Microsoft / Office 365
 -



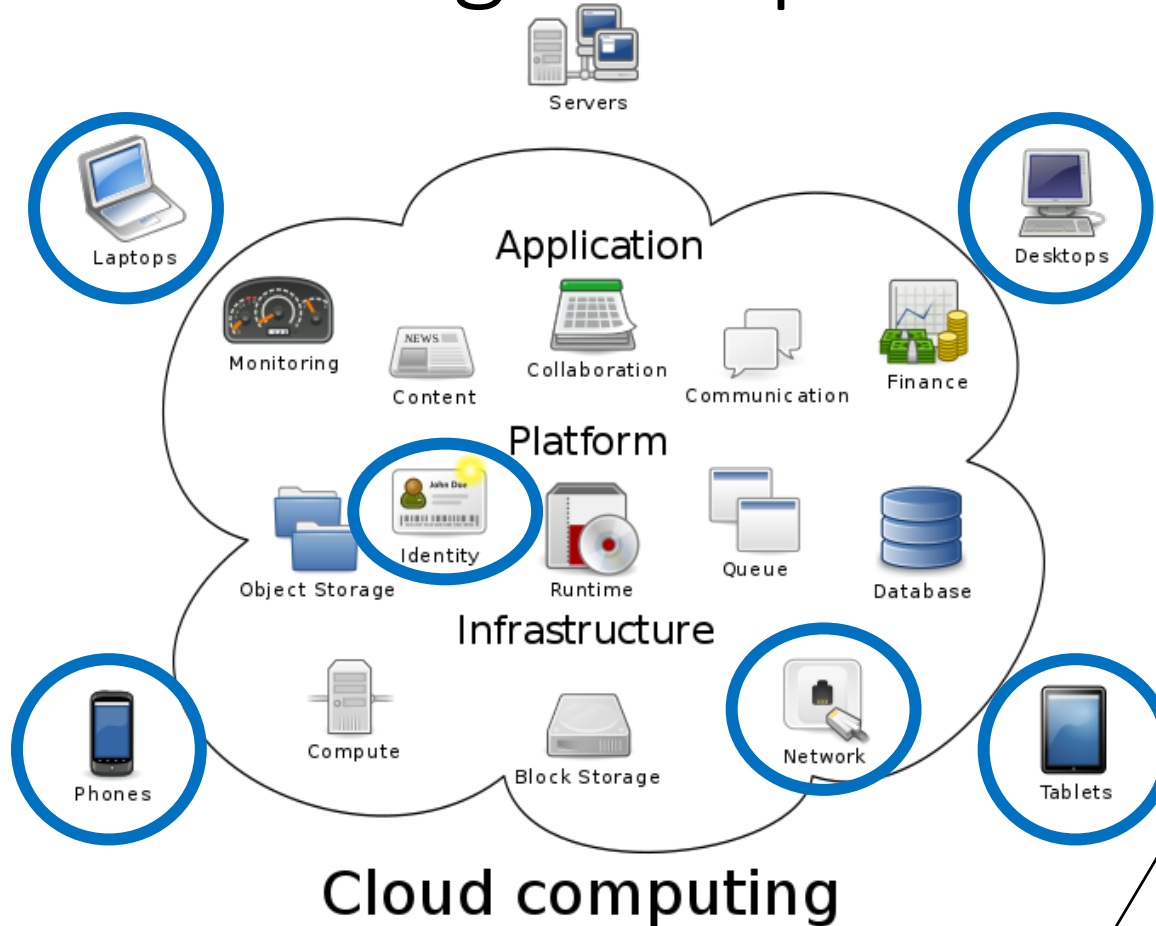
[#bcmuc 2017"](#) by [giesing](#) is licensed under [CC BY 2.0](#)

Compliance-Traum Public Cloud

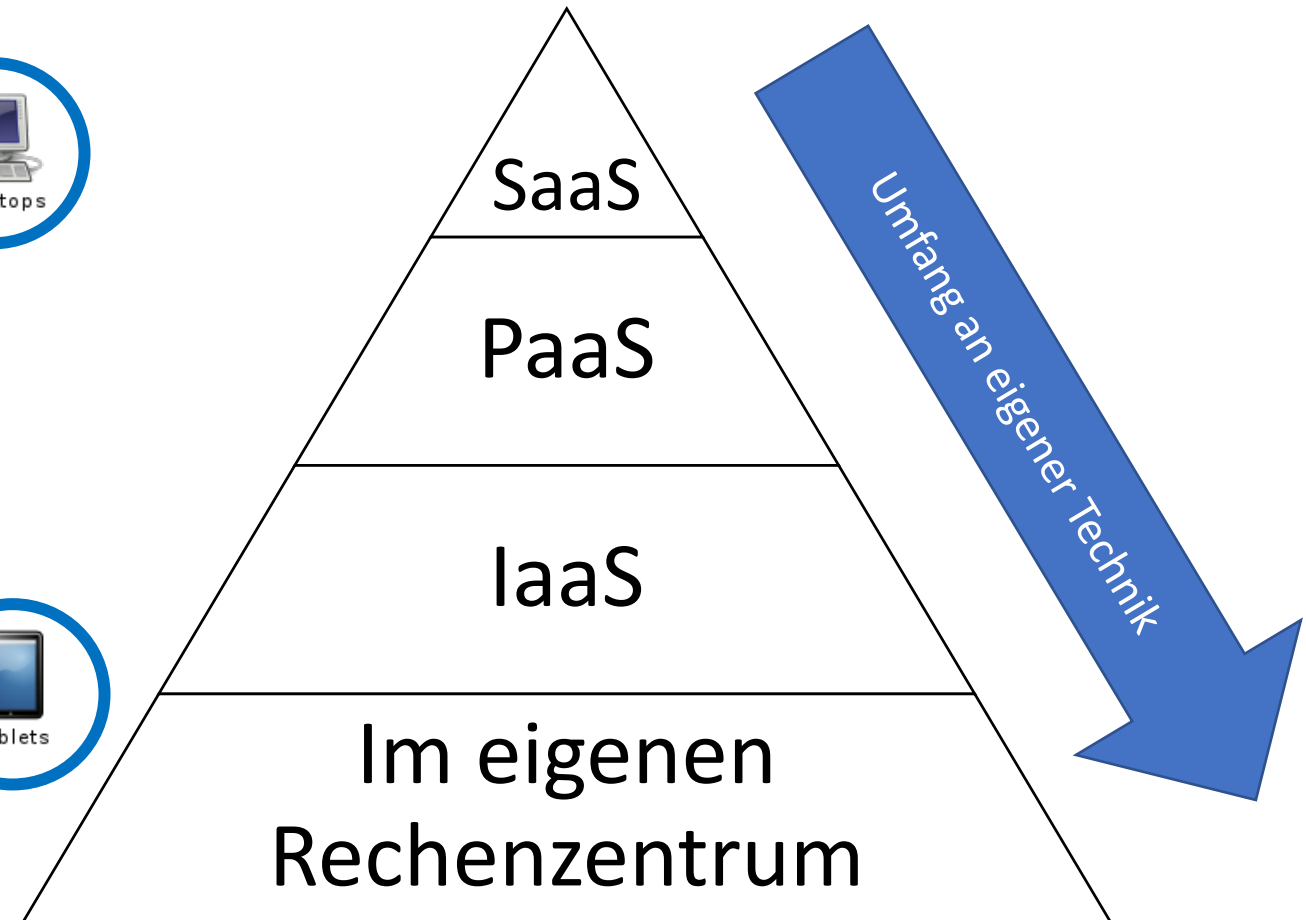
- Modernste Rechenzentren
- Datenklassifizierung durchsetzbar
- Kontrolle jedes Datenzugriffes
- Kontrolle jedes Datenflusses
- Profitieren von den CERT- und SOC-Teams der Anbieter
- Übernahme der Kontrollen für Sicherheitszertifizierungen
- ...



Zuständigkeitssphären



Quelle: [Wikimedia Commons](#) CC BY-SA 3.0



Digitale Souveränität = Art. 33 Abs. 4 GG

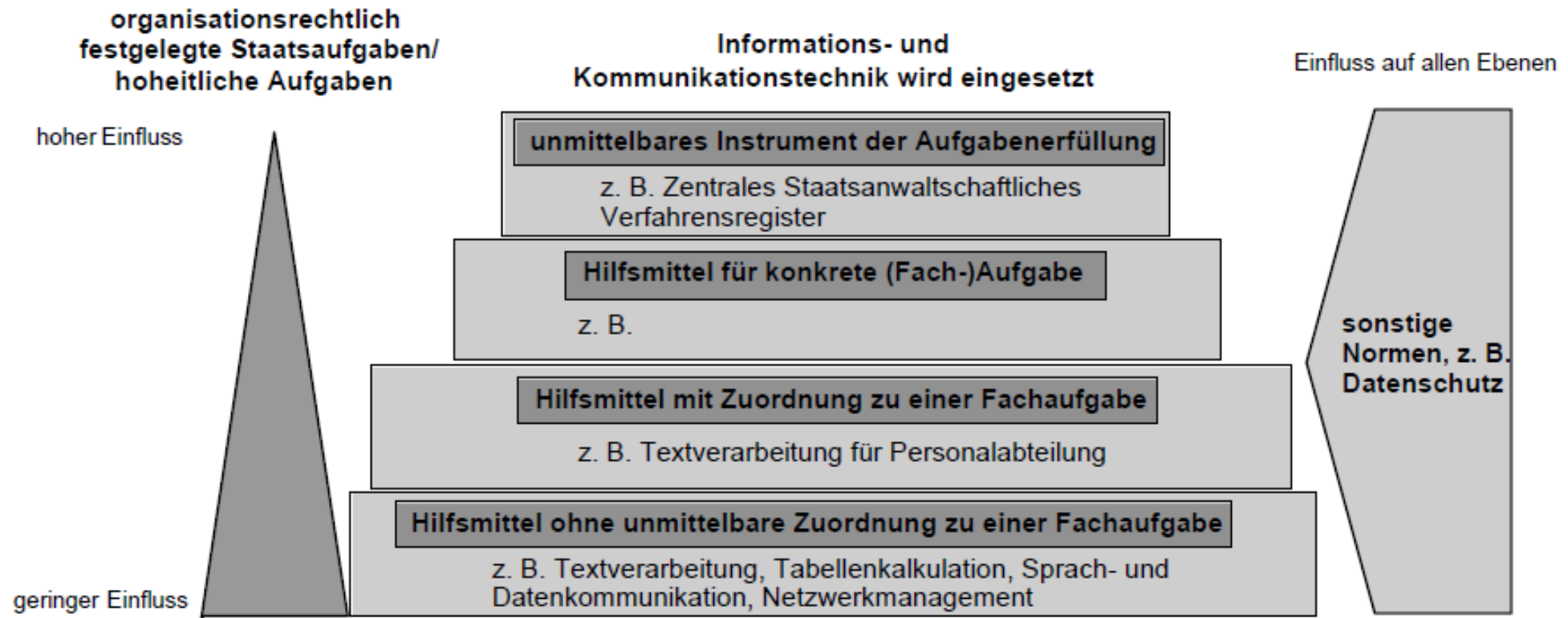


Abbildung 1: Einfluss hoheitlicher Aufgaben und sonstiger Normen auf das LuK-Outsourcing

Quelle: [Leitsätze der Rechnungshöfe für die Prüfung von LuK-Outsourcing](#) S. 6

Rechtlicher Rahmen für die Cloud (vereinfacht)

Souveränität (Art. 33 Abs. 4 GG)

Haushaltsrecht

Datenschutz und Mitbestimmung

Informationssicherheit

Art. 7 und
34 BayHO

Rechnungs-
prüfung

Ort des
Daten-
zugriffs

Umfang der
Auftrags-
verarbeitung

Bes. Daten

Dienst-
Verein-
barung

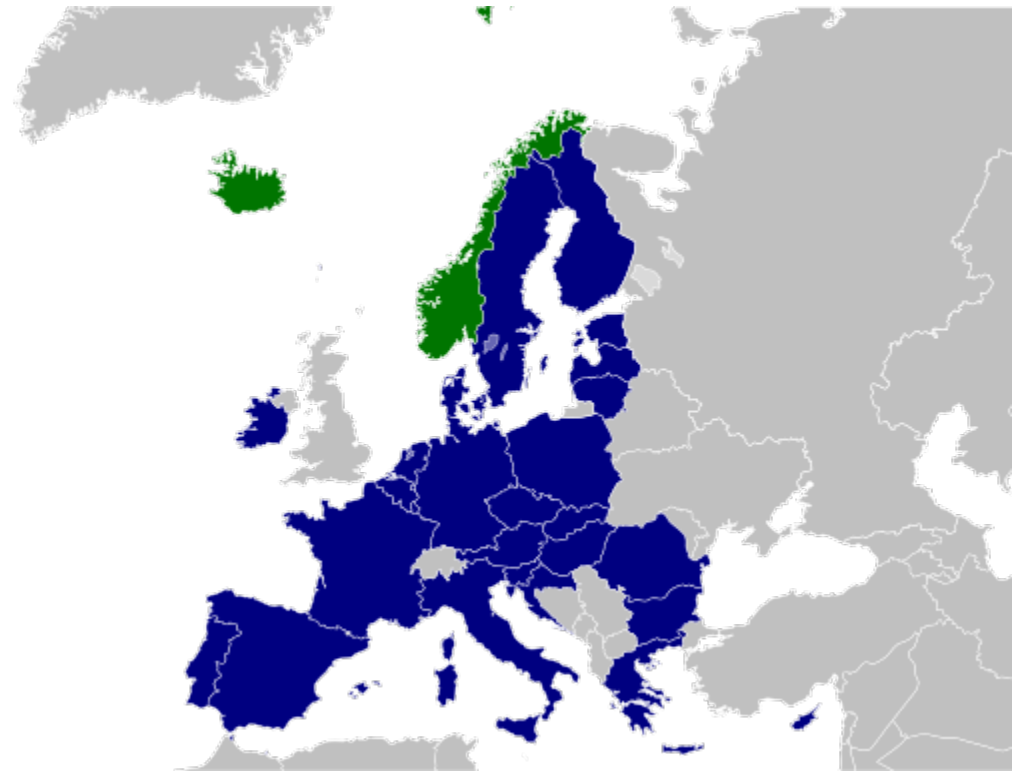
BSI
Standards

Geheimnis-
Schutz

Der Europäische Wirtschaftsraum

Einige Regelungen wie etwa die Datenschutzgrundverordnung gelten über die EU hinaus für den europäischen Wirtschaftsraum.

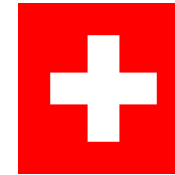
- EU
- Noch UK (wohl bis 31.12.2020)
- Norwegen
- Island
- Lichtenstein



Lösung unter des DSGVO

- Auftragsverarbeiter ist Empfänger aber kein Dritter
- Auftragsverarbeitung eine zulässige Spielform der Datenverarbeitung
- Internationale Datenübermittlungen benötigen zusätzliche Garantien
 - Sichere Drittstaaten oder „Unternehmen“
 - Standarddatenschutzklauseln
 - Die weiteren rechtlichen Ausnahmen sind im Dienstleistungsbereich nicht praktikabel.

Drittländer und Unternehmen mit angemessen „Datenschutz“



https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en



Unsicherheiten

- Public Cloud auf der Blacklist der Bayerischen Landesbeauftragten für Datenschutz
- Software und Plattform as a Service nur bei mit gemeinsamer Verantwortlichkeit möglich?
- Auftragsverarbeitung muss u.a. Art. 28 und 29 DSGVO erfüllen
- Gültigkeit der noch geltenden Standardvertragsklauseln
- Gültigkeit des EU-US-Privacy Shield
- Unvereinbarkeit von Art. 48 DSGVO etwa mit dem CLOUD-Act

Definitionstrick für die Auftragsverarbeitung

AWS:

“Customer Data” means the “personal data” (as defined in the GDPR) that is uploaded to the Services under Customer’s AWS accounts

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Microsoft:

“Customer Data” means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Support Data.

<http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=English>

Google:

“Customer Data” means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

https://gsuite.google.com/terms/dpa_terms.html

Geheimnisschutz

Geheimnisschutz ist Pflicht!

- Für öffentliche Stellen u.a. § 203 StGB
 - ✓ Erfordert Vertraulichkeitsvereinbarungen mit den Dienstleistern
 - ✓ Fehlende Vertraulichkeitsvereinbarung ist strafbewährt
 - ✓ Mindestens Vertraulichkeitsvereinbarungen wie in den EVB-IT
 - ✓ Optimal nach Mustern wie Bitkom
- Für nicht öffentliche Stellen wegen Geheimnisschutzgesetz
 - ✓ Fehlenden Maßnahmen zum Schutz von Geheimnissen führen zum Wegfall des gesetzlichen Geheimnisschutzes
- Geheimnisschutz bei Erforderlichkeit mit technischen Schutzmaßnahmen ergänzen

Rechtliche Vorgaben für Bundesbehörden

- IT-Planungsrat
 - [Entscheidung 2016/35 - Cloud-Computing](#)
- Public Cloud
 - [Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Nutzung externer Cloud-Dienste in der Bundesverwaltung](#)
- Cloud Mitnutzung
 - [Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG zur Mitnutzung externer Cloud-Dienste in der Bundesverwaltung](#)
 - [Umsetzungshinweise zu den Mindeststandards des BSI zur Nutzung und Mitnutzung externer Cloud-Dienste nach § 8 Abs. 1 BSIG](#)

Und wenn ich keine Bundesbehörde bin?

- Für Bayern Art. 11 Abs. 1 BayEGovG
 - ➔ Auftragskontrolle und Festlegung von technischen und organisatorischen Maßnahmen erforderlich
 - ➔ Standards in der Informationssicherheit als Maßstab
- Regelungen zur Cloud-Mitnutzung und BSI C5 Empfehlungen
 - Nicht Berücksichtigung bringt u.U. Haftungsrisiken
- Einrichtungen, die kritische Infrastruktur sind, etwa im Bereich Wasser oder Energie können noch zusätzlichen Regeln unterliegen.

Beschaffung

- Noch kein wirklich passender EVB-IT-Vertrag!
- Denken Sie nicht an Leuchttürme sondern an das Brot- und Buttergeschäft!
- Behalten Sie die Datenhoheit über die Finanzströme!
- Cloud hat außerhalb von SaaS noch keine echte Flatrates und ist Pay as Go!
- SLA bringen keinen Schadensersatz z.B. für eigene Aufwände bei Störungen!
- Definieren Sie „höhere Gewalt“ in den Verträgen nicht zu großzügig!
- Für einen rechtssicheren Rahmen helfen die gemeinsamen Cloudausschreibungen über das Sprungbrett DFN.

Grenzen? der Public Cloud: Zwei Beispiele

Steuerrecht

Bisher: Speicherung grundsätzlich in Deutschland.

Denkbar: Auslegung mit Bezug zur Technik, d.h. Zugreifbarkeit und „Schlüssel“ müssen durch den Steuerschuldner sichergestellt sein.

Neu: Ohne Genehmigung im EWR
➔ Freier Fluss von Daten

Personalakten

Art. 108 BayBG

Grundsätzlich kein Outsourcing

Außer wenn wesentlich wirtschaftlicher und wenn, dann

- bei anderen öffentlichen Stellen
- Gesonderte Prüfung der Erforderlichkeit
- bei Nicht-öffentlichen Stellen nur nach Verpflichtung gemäß dem Verpflichtungsgesetz

Zusammenfassung

- Verstehen Sie die Public Cloud, bevor sie diese nutzen!
 - Es kann genau so viel falsch laufen, wie in der eigenen IT, nur sie sind dort viel exponierter.
 - Kennen Sie die Grenzen, was rechtlich in die Public Cloud darf.
- Auch Hochschulen können die Public Cloud nutzen!
 - U.a. Cloud Act steht noch im Widerspruch zum geltenden Datenschutzrecht.
 - Leitung kann sich zum Tragen des Risikos entscheiden, etwa weil Public Cloud Lösung in der Summe mehr Compliance schafft.
 - Eine Datenschutzfolgeabschätzung kann u.U. erforderlich sein.
 - Sie müssen wieder aussteigen können.
- Verträge bergen noch Fallstricke!
 - Gehen Sie nicht alleine, sondern gemeinsam unter dem Schirm eines großen Rahmenvertrages.

Checkliste

- Funktionsweise des Dienstes verstehen lernen
- Rechtliche Implikationen der einzelnen Funktionen prüfen
- Lösungen und Pflichten
 - Datensparsame Personenprofile
 - Verschlüsselung durch Drittdienste
 - Einbinden etwa von HSM-Lösungen
 - Kontrolle von Supportzugriffen
 - Bedarf der Datenschutzfolgeabschätzung
 - Wirtschaftlichkeitsbetrachtungen

Checkliste II

- Datenklassifikation ist der Schlüssel
- Bezahlung erfolgt mit Geld und (statistischer) Nutzungsanalyse (Leistungsentscheidung!)
- Datenschutzinformation an alle Nutzenden
- Effektive interne Bestell- und Freigabeprozesse für Lizenzen und Ressourcen
- Beteiligung des Personalrates
- Bevorzugung eines Multi-Cloudansatzes
- Lokales Backup der Daten (einschließlich Konfiguration)
- Sicherheitskonzept (Intern + Anbieter)
- Barrierefreiheit nicht vergessen

Vielen Dank für Ihre Aufmerksamkeit!



Kontakt:

Johannes Nehlsen

Tel.: 0931/31-84217

Johannes.nehlsen@uni-wuerzburg.de

<https://www.rz.uni-wuerzburg.de/dienste/it-recht>

Twitter privat: @JoNehlsen

Nehlsen – Public Cloud

Dieses Werk ohne Zitate, geschützte Marken, Icons und unwesentlichem Beiwerk ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).