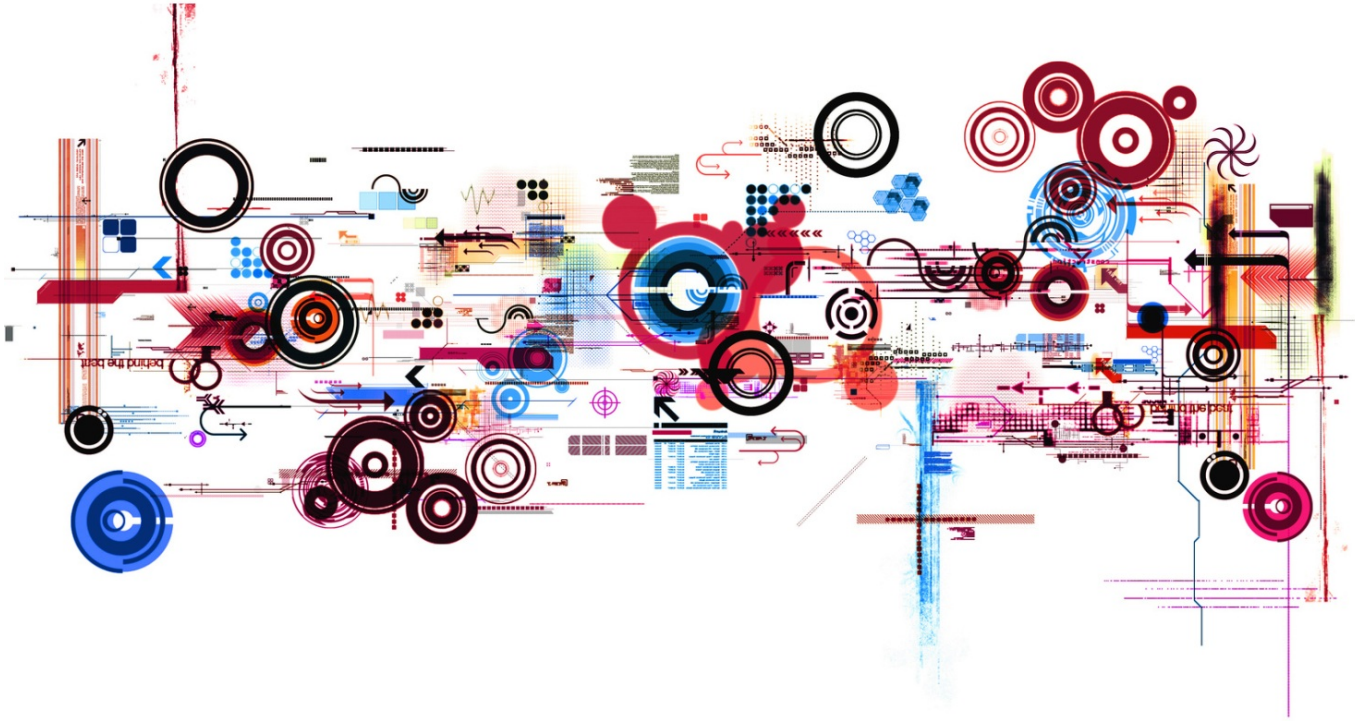
Cloud-Services: AWS-Nutzung

Chancen und Risiken, Vertragsgestaltung und Datenschutz



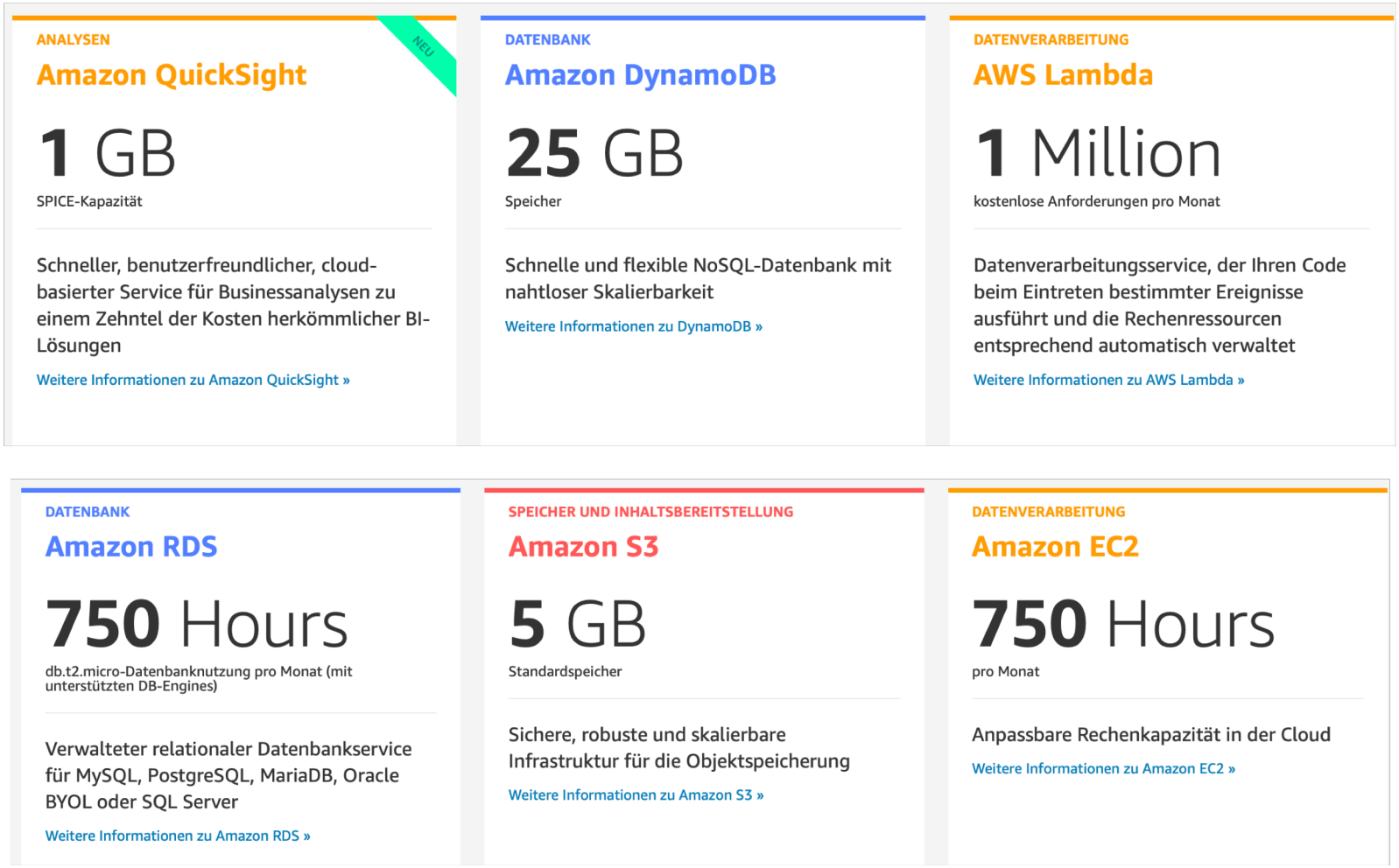
AWS – ist was?

- Cloud basierte Services, RZ, Datensicherheit, Datenschutz, Server, Tools, Speicher, skalierbar, individuell nutzbar
- US-Vertragspartner (Inc.), auch wenn Kunde in Deutschland
- Bietet letztlich nur Infrastruktur und Verfügbarkeit, der Kunde ist für seine „Systeme“ i.S.v. Anwendung, Daten, Sicherheitsniveau seiner Installation selbst verantwortlich
- Bietet weltweit RZ an, auch auf Wunsch des Kunden beschränkt auf bestimmte Regionen, z.B. Frankfurt mit Parallelregion Irland (was auch zugesichert wird)
- Siehe aws.amazon.com

AWS – nutzt wer?

- Private Kunden für Standardanwendungen, z.B. Dropbox
- Unternehmenskunden für ihre Anwendungen
- Netflix, Foursquare, Reddit
- IT-Dienstleister als Standardinfrastruktur, z.B. Salesforce (Vertriebssystem und CRM), GfK (als backup-System)
- HRworks (Personalverwaltungssystem)
- Almabase: führende britische Software für Schulverwaltung und Alumnikontakte einschließlich Spendensammeln
- Workday: führende US HR-Software für die Nutzung von workday in der public cloud, bietet aber auch eine private cloud Lösung ohne AWS an.

AWS – leistet?


ANALYSEN
Amazon QuickSight
NEU
1 GB
SPICE-Kapazität
Schneller, benutzerfreundlicher, cloud-basierter Service für Businessanalysen zu einem Zehntel der Kosten herkömmlicher BI-Lösungen
Weitere Informationen zu Amazon QuickSight »
DATENBANK
Amazon DynamoDB
25 GB
Speicher
Schnelle und flexible NoSQL-Datenbank mit nahtloser Skalierbarkeit
Weitere Informationen zu DynamoDB »
DATENVERARBEITUNG
AWS Lambda
1 Million
kostenlose Anforderungen pro Monat
Datenverarbeitungsservice, der Ihren Code beim Eintreten bestimmter Ereignisse ausführt und die Rechenressourcen entsprechend automatisch verwaltet
Weitere Informationen zu AWS Lambda »
DATENBANK
Amazon RDS
750 Hours
db.t2.micro-Datenbanknutzung pro Monat (mit unterstützten DB-Engines)
Verwalteter relationaler Datenbankservice für MySQL, PostgreSQL, MariaDB, Oracle BYOL oder SQL Server
Weitere Informationen zu Amazon RDS »
SPEICHER UND INHALTSBEREITSTELLUNG
Amazon S3
5 GB
Standardspeicher
Sichere, robuste und skalierbare Infrastruktur für die Objektspeicherung
Weitere Informationen zu Amazon S3 »
DATENVERARBEITUNG
Amazon EC2
750 Hours
pro Monat
Anpassbare Rechenkapazität in der Cloud
Weitere Informationen zu Amazon EC2 »

AWS Zielgruppen + Erfolgsgeschichten

AWS und Cloud Computing

- Was ist Cloud Computing?
- Was ist Caching?
- Was ist NoSQL?
- Was ist DevOps?
- Was ist Docker?
- Produkte und Services
- Kundenerfolg
- Economics Center
- Architekturzentrum
- Sicherheitszentrum
- Neuerungen
- Whitepapers
- AWS-Blog
- Ereignisse
- Nachhaltige Energie
- Pressemitteilungen
- AWS in den Medien
- Analystenberichte
- Rechtlicher Hinweis

Lösungen

- Websites und Websitehosting
- Unternehmensanwendungen
- Sicherung und Wiederherstellung
- Notfallwiederherstellung
- Datenarchiv
- DevOps
- Serverlose Datenverarbeitung
- Big Data
- High Performance Computing
- Services für Mobilgeräte
- Digitales Marketing
- Entwicklung von Spielen
- Digitale Medien
- Behörden und Bildungswesen
- Gesundheitswesen
- Finanzdienstleistungen
- Windows in AWS
- Einzelhandel
- Strom und Energieversorgung
- Öl und Gas
- Kraftfahrzeuge
- Blockchain
- Fertigung

Angel MedFlight salesforce

Angel MedFlight und Salesforce
Angel MedFlight arbeitet mit Familien und Gesundheitsdienstleistern zusammen, um Patienten von überall auf der Welt für die erforderliche lebensverändernde Pflege sicher zu transportieren. Für das Angel MedFlight-Team ist ein schnelles Handeln entscheidend, um ein optimales Ergebnis für den Patienten zu erzielen. Das Unternehmen nutzt die Salesforce Marketing Cloud und Sales Cloud, um Patientendaten zu sammeln und viele Aspekte des Unternehmens zu unterstützen.

NASA

NASA & Infozen

To better share its achievements with the public, NASA turned to **InfoZen**, an Advanced Consulting Partner of the AWS Partner Network (APN) to consolidate its vast array of images and videos. Now NASA is able to bring the universe to the publics' fingertips.

Nach Branche

Kraftfahrzeuge
Entwickeln Sie vernetzte Erfahrungen und beschleunigen Sie die Markteinführungszeit für jeden Kontaktpunkt des Kundenerlebnisses

Digitales Marketing
Betreiben Sie Ihr digitales Marketing-Geschäft mit flexiblen, hochskalierbaren, elastischen und kostengünstigen Lösungen als Fundament

Bildung
Lösungen für bessere Lehr- und Lernumgebungen, engere Studentenbeziehungen, optimale Lernergebnisse und moderne, unternehmensweite IT-Infrastruktur

Unternehmensanwendungen
Eine ausgereifte Reihe von Services speziell für die besonderen Anforderungen großer Unternehmen

Finanzdienstleistungen
Entwicklung sicherer und innovativer Lösungen zur Steigerung des Unternehmenswerts und des Werts eines Unternehmens für seine Kunden

Gaming
Services für die Entwicklung von Spielen aller Genres, auf allen Plattformen, von AAA-Spielen bis zu kleinen unabhängigen Studios

AWS – wo liegt das Problem?

- Anbieter ist die Amazon Webservices Inc.
- Es gibt keine europäische Entity, mit der ein Vertrag geschlossen werden könnte -> AWS unterliegt der US-Aufsicht und US-Einflussnahme (DHS US Department of Homeland Security)
- Cloud-basierte Lösung und weltweit verfügbar
- Services werden nach SLA 24/7 follow the sun erbracht, d.h. Support von außerhalb der EU ist nicht auszuschließen

AWS – Verbreitung

Region und Anzahl der Availability Zones

USA Ost
Nord-Virginia (6), Ohio (3)

USA West
Nordkalifornien (3), Oregon (3)

Asien-Pazifik
Mumbai (2), Seoul (2), Singapur (3), Sydney (3), Tokio (4), Osaka-Lokal (1)

Kanada
Zentral (2)

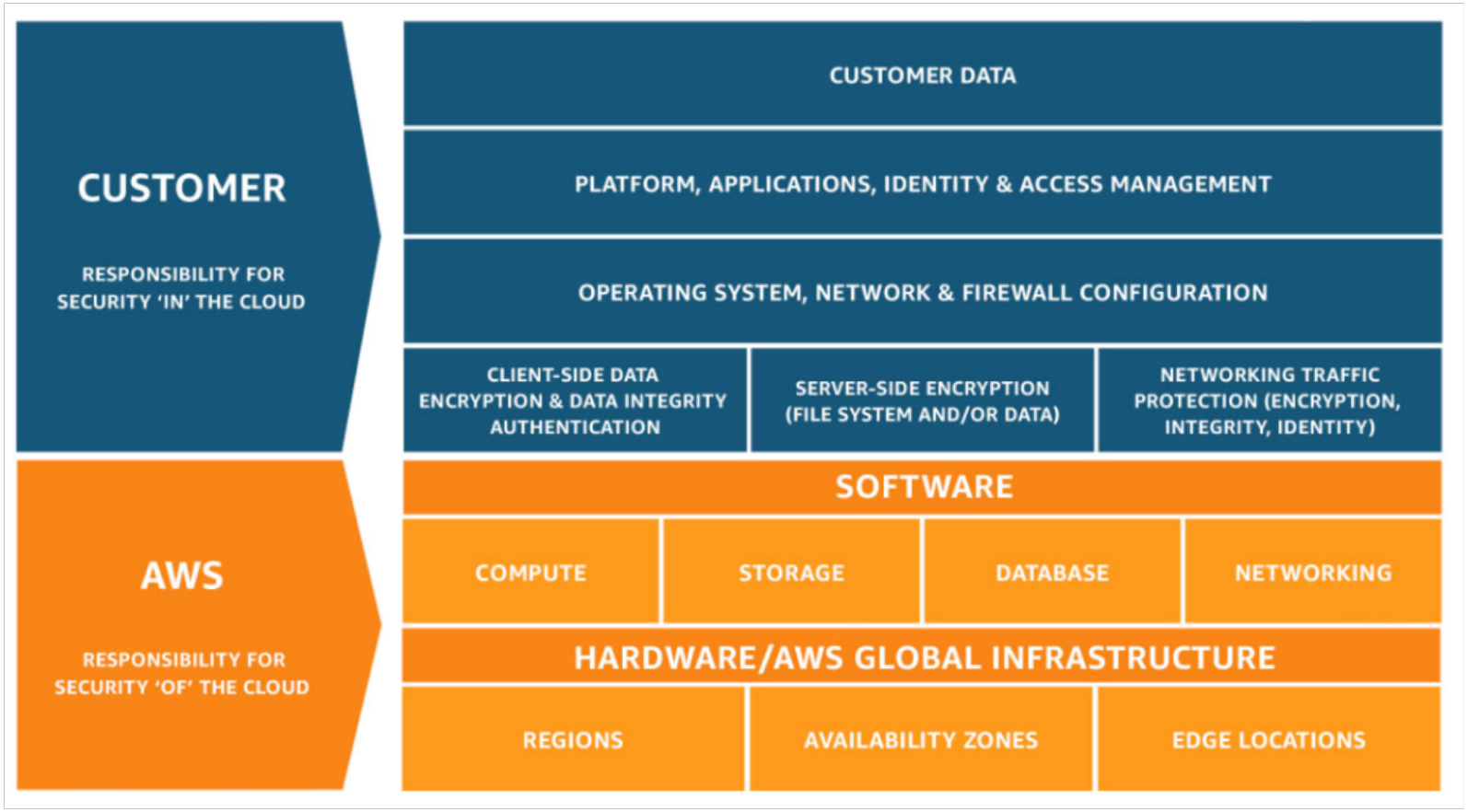
China
Peking (3), Ningxia (2)

Europa
Frankfurt (3), Irland (3), London (3), Paris (3)

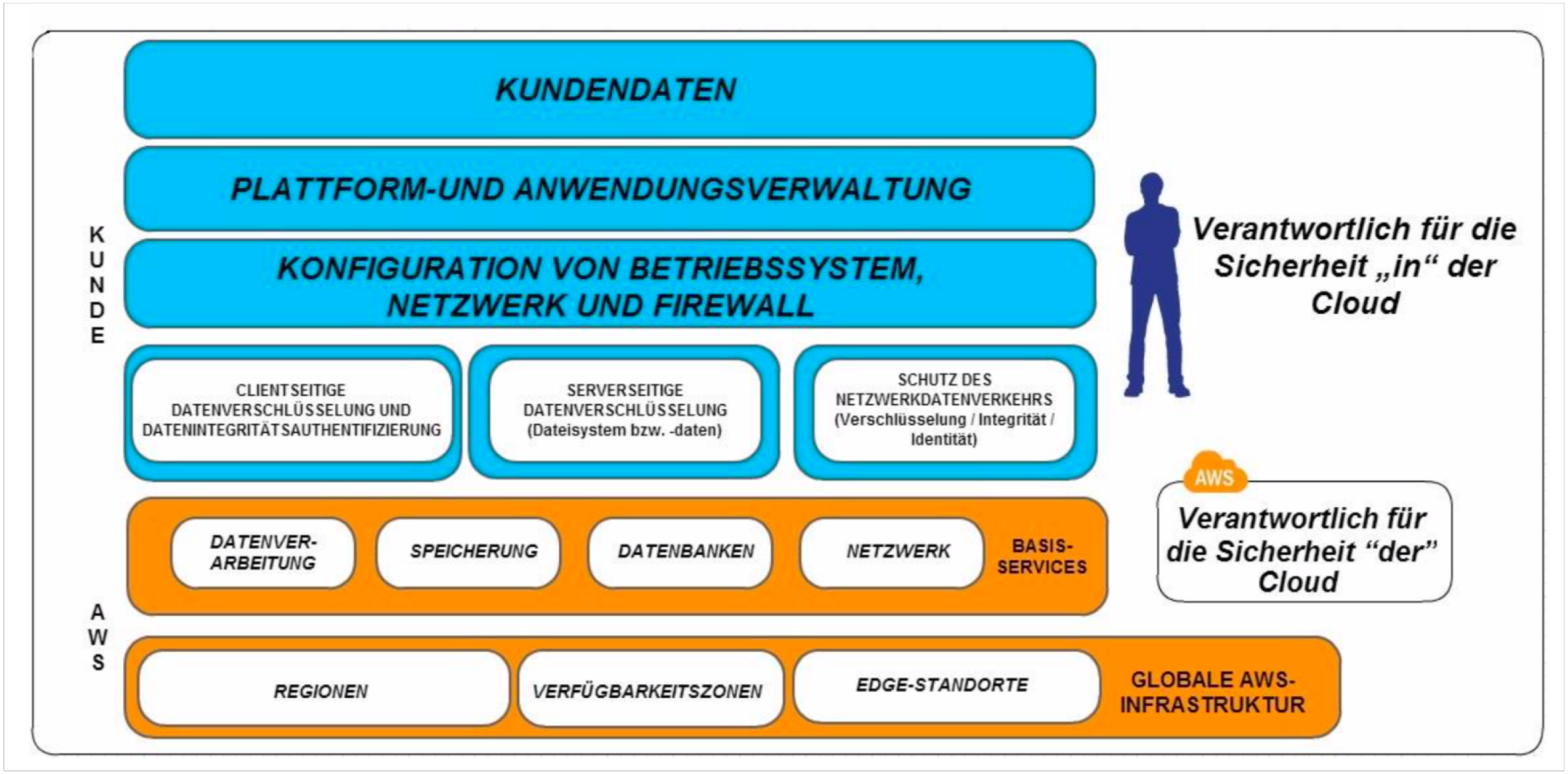
Südamerika
São Paulo (3)

AWS GovCloud (US-West) (3)

AWS Verantwortlichkeitsmatrix



AWS Verantwortlichkeitsmatrix



AWS Technik: Zugriffe

Amazon Web Services – **Übersicht über die Sicherheitsprozesse**

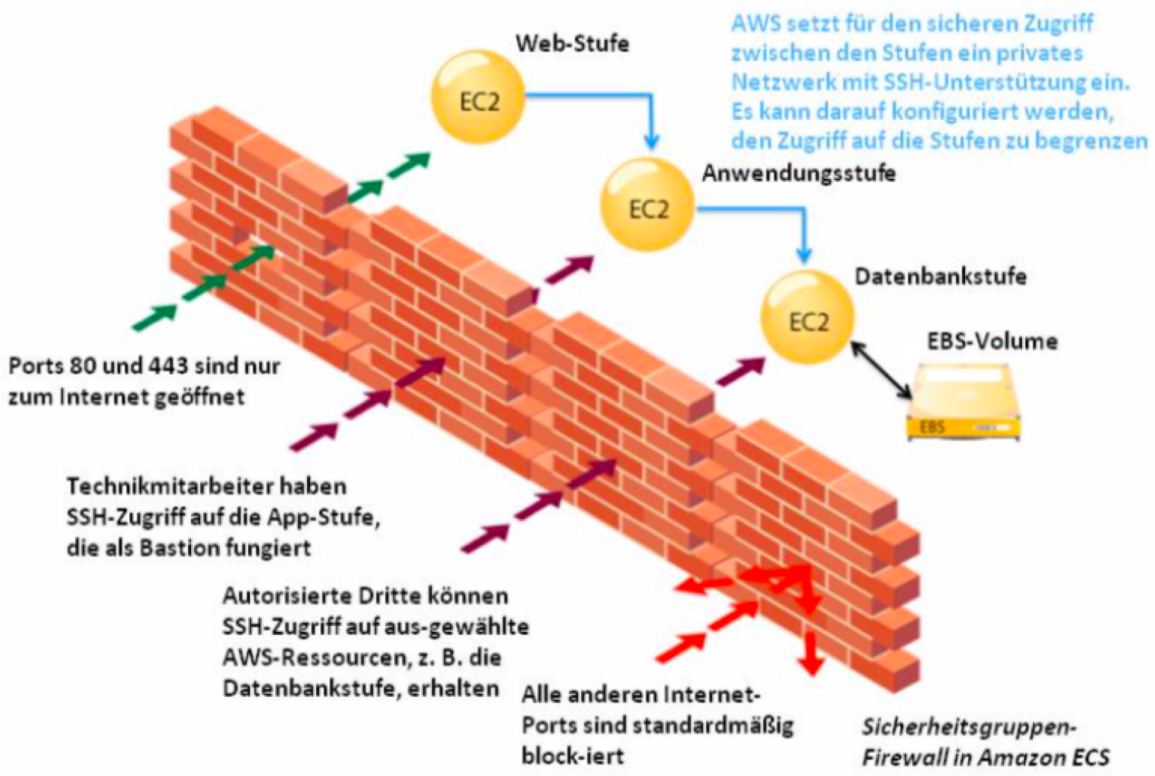


Abbildung 3: Sicherheitsgruppen-Firewall in Amazon EC2

AWS Zugriffe: Bastion Host

Unternehmenstrennung bei Amazon

Für den logischen Zugriff wird das AWS-Produktivnetzwerk vom Amazon-Unternehmensnetzwerk durch einen Reihe von Maßnahmen der Netzwerksicherheit- und -trennung abgegrenzt. AWS-Entwickler und Administratoren des Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, um diese zu verwalten, müssen ausdrücklich Zugriff über das AWS-Ticketing-System beantragen. Alle Anträge werden vom entsprechenden Service-Owner geprüft und genehmigt.

Zugelassenes AWS-Personal stellt dann eine Verbindung zum AWS-Netzwerk durch einen Bastions-Host her, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten einschränkt und alle Aktivitäten zur Sicherheitsüberprüfung protokolliert. Der Zugriff auf Bastions-Hosts erfordert für alle Benutzerkonten auf dem Host eine Authentifizierung durch einen öffentlichen SSH-Schlüssel. Weitere Informationen über den logischen Zugriff für AWS-Entwickler und -Administratoren finden Sie nachfolgend unter *AWS-Zugriff*.

Bastions-Host: Ein Computer, der dafür konfiguriert wurde, Angriffen standzuhalten. Er wird in der Regel auf der äußeren/öffentlichen Seite einer demilitarisierten Zone (DMZ) oder außerhalb der Firewall platziert. Sie können eine Amazon EC2-Instanz als SSH-Bastion aufsetzen indem Sie ein öffentliches Subnetzes als Teil einer Amazon VPC einrichten.

AWS-Zugriff

Das AWS-Produktivnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktivnetzwerk eine SSH public-key Authentifizierung mit einem Bastions-Host erfordert.

AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich Zugriff über das AWS-Zugriffsverwaltungssystem beantragen. Alle Anträge werden von der jeweils zuständigen Person geprüft und genehmigt.

Sicherheitstechnik für die Kunden „in der cloud“

	Key Location	Key Management	S3	EBS	Glacier	Notes
No Encryption	None	None	Yes	Yes	No	Not recommended as protection is free of charge on AWS
AWS Base Encryption	AWS	AWS	Yes*		Yes	Minimum recommended standard.
AWS Encryption with KMS	AWS	Shared AWS / Customer	Yes		No	Customers can select their Master-Key, key rotation is possible. Key activity is shown in AWS CloudTrail
CloudHSM BasedEncryption	Customer controlled HSM in AWS Datacenters	Customer	With Customer Application	With Customer Application	N/A	Needs integration into Applications/Customer operating Systems
Own CloudHSM on DX	HSM on Customer Premises	Customer	With Customer Application	With Customer Application	N/A	Needs integration into Applications/Customer operating Systems

Gesetzliche Grundlagen

- DSGVO
- BDSG (neu)
- Orientierungshilfe Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0 Stand 09.10.2014

Was verlangt das Gesetz? Rückblick und heute

- Ausgangspunkt: TOM des Auftragsverarbeiters: sind vom Auftraggeber festzulegen und zu überprüfen
- BDSG (alt): § 9a: „ Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.
- BDSG (neu): keine eigenen Regelungen
- DSGVO: Art 42 und 43, Zertifizierungen und Zertifizierungsstellen

Forderungen der DSGVO

- Art 24 DSGVO: (1) Der **Verantwortliche** setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
- (3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.
- Art 28 DSGVO (5): Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen **Auftragsverarbeiter** kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

Forderungen der DSGVO

- EG 81: Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die - insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen - hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen - auch für die Sicherheit der Verarbeitung - getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter **kann als Faktor** herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.
- EG 100: Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

Forderungen der DSGVO

- Art. 42 DSGVO, Zertifizierungen:

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

(4) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.

- Art 43 DSGVO, Zertifizierungsstellen

Sinn und Bedeutung von Zertifikaten

- Der Cloud-Anbieter unterwirft sich einem Satz von Anforderungen und lässt sich von einem **unabhängigen Dritten** auf die Einhaltung dieser Anforderungen prüfen.
- Die Prüfung erfolgt anhand eines **einheitlichen Kriterienkatalogs**, der **regelmäßig weiterzuentwickeln** und dem Stand der Technik anzupassen ist. Die Prüfkriterien sind entweder in **Normen** oder durch die Zertifizierungsstelle festzulegen, was bei unabhängigen Stellen i.d.R. schneller gelingt als in einem Gesetzgebungsverfahren.
- Die Prüfung folgt dem für das Zertifikat/Testat zugrunde gelegten **Auditschema** und das Prüfungsergebnis wird in einem festgelegten Format festgehalten und ggf. veröffentlicht.
- Der Anwender (oder Kunde) kann dann seine Anforderungen mit denen dem Zertifikat/Testat zugrunde liegenden abgleichen und entscheiden, ob die eigenen Anforderungen dadurch abgedeckt sind.
- Zertifikate und Testate dienen aber auch dazu, Vertrauen aufzubauen, denn der (Cloud-)Anbieter macht einem Externen die eigenen Sicherheitsmaßnahmen transparent und veröffentlicht das Ergebnis oder zumindest Teile davon.

Probleme mit Zertifikaten (derzeit)

- Gesetzlichen Vorgaben für die Erstellung, Prüfung und Beurteilung derartiger Zertifikate fehlen.
- Sämtliche auf dem Markt befindlichen Testate, Zertifizierungen oder allgemeine Beurteilungen greifen auf selbstdefinierte Maßstäbe zurück.
- Gerade im Online-Bereich sind Datenschutz- und Datensicherheitssiegel sehr heterogen, es mangelt ihnen häufig an allgemeinen Standards, Bekanntheit, Validität und Nutzbarkeit.
- Im Januar 2016 existierten allein in Deutschland 41 unterschiedliche Zertifikate und Systeme.
- Auch die Zugrundelegung anerkannter, wenngleich außerhalb des Gesetzes normierter Standards wie ISO oder DIN ändern hieran nichts, da es für die Bewertung des materiellen Datenschutzniveaus an konkreten Maßstäben fehlt.
- International geht die Beurteilungsmöglichkeit für einen Anwender gegen Null, wenn es keine einheitlichen EU-weiten Standards gibt. Staatsgrenzen dürfen bei einer Auditierung aber keine Auswirkungen auf die Aussagekraft eines Zertifikates haben.

Zertifizierungen von AWS

- **ISO 27001**, technische Maßnahmen: Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Die Norm spezifiziert Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen adaptiert werden sollen.
- **ISO 27017**, Sicherheit in der Cloud: Die ISO/IEC 27017 ist eine internationale Norm zur Absicherung von Cloud-Services. In dieser Norm sind spezifische Empfehlungen für die Anbieter von Cloud-Dienstleistungen definiert. Der Standard gehört zur Normenfamilie der ISO/IEC 27001, die Anforderungen der ISO/IEC 27017 sind speziell für die Anbieter von Cloud-Dienstleistungen zugeschnitten worden. Darüber hinaus spezifiziert die ISO/IEC 27017 die Beziehung zwischen Kunden und Cloud-Anbietern.
- **ISO 27018**, Datenschutz in der Cloud: ISO 27018 ist ein Verhaltenskodex für den Schutz persönlicher Daten in der Cloud. Er basiert auf dem Informationssicherheitsstandard ISO 27002 und dient als Leitfaden für die Implementierung von ISO 27002-Steuerungen, die für personenbezogene Daten, anhand derer eine Person eindeutig identifiziert werden kann, in der öffentlichen Cloud gelten. Der Standard bietet zusätzliche Kontrollen und Richtlinien für die Schutzanforderungen von personenbezogenen Daten.

Nachweise von AWS für die Kunden

- **SOC 1**: Ein Bericht nach Service Organization Control 1 oder SOC 1 (ausgesprochen "Sock One") ist eine schriftliche Dokumentation interner Kontrollmechanismen, die höchstwahrscheinlich für eine Überprüfung der Finanzberichterstattung eines Kunden relevant sind. SOC 1 wird in Typ 1 und Typ 2-Berichte unterteilt. **Typ 1** berichtet darüber, **wie angemessen die Kontrollmechanismen einer Service-Organisation zu einem bestimmten Zeitpunkt bzw. Datum** sind, während Typ 2 eine Aussage zur Wirksamkeit der Kontrollmechanismen über einen längeren Zeitraum trifft. SOC 1-Berichte werden von einem Service-Auditor erstellt. Sie erfüllen die Anforderungen gemäß SSAE 16.
- **SOC 2**: SOC 2, ausgesprochen „Sock Two“ und offiziell bekannt als Service Organization Control 2, ist ein Standard, gemäß dem Service-Organisationen Berichte zum Status bestimmter interner Kontroll-Parameter erstellen. Diese umfassen Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz. Der Standard wurde nach den AICPA Trust Services Principles and Criteria erstellt.
- **SOC 3**: SOC 3 berichtet über dieselben Informationen wie ein SOC 2-Bericht. Der Hauptunterschied zwischen beiden besteht darin, dass **SOC 3 für ein allgemeines Publikum vorgesehen ist. Die Berichte sind also kürzer und gehen nicht so sehr ins Detail wie SOC 2-Berichte**, die an ein informiertes Publikum aus interessierten Parteien verteilt werden. Aufgrund ihrer allgemeineren Natur können SOC 3-Berichte offen verbreitet und etwa – mit einem Siegel, das die Einhaltung bestätigt – auf der Webseite des Unternehmens veröffentlicht werden.
- **PCI DSS Level 1**: Der Payment Card Industry Data Security Standard, üblicherweise abgekürzt mit PCI bzw. PCI-DSS, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.

Anforderungen der Aufsichtsbehörden

Zertifikate und Vor-Ort Prüfungen

Dem Cloud-Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Cloud-Anbieters verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte IT-Sicherheitsstandards eingehalten werden. Die Lösung kann darin bestehen, dass der Cloud-Anbieter sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der IT-Sicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft. Das **Vorliegen von Zertifikaten entbindet den Cloud-Anwender aber nicht von seinen Kontrollpflichten nach § 11 Abs. 2 Satz 4 BDSG, da die bloße Berufung auf eine Zertifizierung z.B. nach ISO 27001 für den Bereich Datenschutz nicht aussagekräftig wäre**. Vielmehr muss sich der Cloud-Anwender anhand der in den Zertifizierungs- bzw. Gütesiegelverfahren erarbeiteten Gutachten, Berichte und Analyseergebnisse darüber Klarheit verschaffen, ob und in welchem Umfang sich der Untersuchungsgegenstand auf **cloudspezifische Datenschutz- und IT-Sicherheitsrisiken** bezieht und dabei die vom Cloud-Anbieter zur Verfügung gestellten Dienste (IaaS, PaaS oder SaaS) geprüft wurden. Es reicht z.B. nicht aus, wenn für den Cloud-Anbieter mit dem Gütesiegel oder der Zertifizierung bescheinigt wurde, dass für einen beliebigen Geschäftsprozess ein Sicherheitskonzept vorliegt.

Anforderungen der Aufsichtsbehörden

Eine Zertifizierung z. B. nach ISO 27001 kann hier als wichtiger Baustein für einen Prüfnachweis dienen, indem das erforderliche Sicherheitsniveau aus Unternehmensperspektive untersucht wurde. Ergänzend muss der Cloud-Anwender vom Cloud- Anbieter aber auch den Nachweis einer unabhängigen Stelle erbringen, dass mit diesem Sicherheitsniveau auch die Datenschutzrisiken für die Betroffenen wirksam und im erforderlichen Maß und Umfang begrenzt werden, was mit einer Zertifizierung nach ISO 27001 gerade nicht bescheinigt wird.

Es geht etwa um die Frage, ob die Betroffenenrechte wie die Rechte auf Auskunft, Löschung, Berichtigung und Sperrung mittels der eingesetzten Hard- und Software auf dem jeweiligen Sicherheitsniveau umgesetzt wurden. Nur vor diesem Hintergrund kann auf Seiten des Cloud-Anwenders bezüglich der beim Cloud-Anbieter getroffenen technisch-organisatorischen Maßnahmen eine Überzeugungsbildung nach § 11 Abs. 2 Satz 4 BDSG stattfinden.

Anforderungen der Aufsichtsbehörden

Im Übrigen dürfen **eigene Kontrollrechte** des Cloud-Anwenders **vertraglich nicht ausgeschlossen werden**, selbst wenn gewollt ist, dass die Auftragskontrolle in der Praxis in aller Regel durch die Vorlage geeigneter Zertifikate ausgeführt werden soll.

Der Auftraggeber muss sich daneben zumindest die rechtliche Möglichkeit vorbehalten, Kontrollen auch selbst (oder durch einen von ihm ausgewählten sachkundigen Dritten) durchzuführen. Mit anderen Worten darf aus den zwischen Cloud-Anbieter und Cloud-Anwender geschlossenen vertraglichen Vereinbarungen nicht hervorgehen, dass die Vorlage von Zertifikaten die **einzige Möglichkeit zur Ausübung der Auftragskontrolle** sein soll. Darauf ist bei der Vertragsgestaltung besonders zu achten, insbesondere dann, wenn der Cloud-Anwender eigene vorformulierte Vertragsbedingungen vorlegt.

Anforderungen der Aufsichtsbehörden

Unterauftragnehmer

Besteht eine Erlaubnis zur Beauftragung von Unter-Anbietern, so müssen im Rahmen der Unterbeauftragung die Vorgaben des Vertrags zwischen Cloud-Anwender und Cloud-Anbieter berücksichtigt werden. Der Cloud-Anbieter muss in diesem Fall vor Beginn der Datenverarbeitung im Rahmen der Unterbeauftragung eine Kontrolle nach § 11 Abs. 2 Satz 4 BDSG vornehmen. Hierfür muss dann derselbe Kontrollmaßstab gelten wie im Verhältnis zwischen Cloud-Anwender und Cloud-Anbieter. Dabei ist zu fordern, dass der Cloud-Anwender die Begründung von Unteraufträgen davon abhängig macht, dass der Cloud-Anbieter entsprechende Vereinbarungen mit dem Unter-Anbieter trifft. Allgemein gilt daher: Zwischen dem Cloud-Anbieter und dem Unterauftragnehmer ist ein Vertrag zu schließen, der die zwischen Cloud-Anwender und Cloud-Anbieter geltenden Vertragsbedingungen widerspiegelt (vgl. WP 196, Nr. 3.3.2, letzter Absatz).

Unter anderem mü**ssen daher im Unterauftrag auch Kontrollrechte des Auftraggebers** selbst gegenüber dem Unterauftragnehmer vorbehalten werden. Selbst wenn gewollt ist, dass die Kontrolle des Unterauftragnehmers in der Regel durch den Cloud-Anbieter (d. h. den Haupt-Auftragnehmer) durchgeführt werden soll, **dürfen eigene Kontrollrechte des Auftraggebers gegenüber Unterauftragnehmern nicht ausgeschlossen werden**; ein solcher Ausschluss wäre mit der sich aus § 11 Abs. 1 Satz 1 BDSG ergebenden datenschutzrechtlichen Verantwortlichkeit des Cloud-Anwenders als Auftraggeber nicht vereinbar.

Aussagen der Stiftung Datenschutz

- Datenschutzbezogene Zertifizierungen

Nach der seit dem 25. Mai 2018 anzuwendenden DSGVO gelten für Zertifizierungsstellen im Datenschutz neue Anforderungen. Für Zertifizierungen im Datenschutzrecht (Bestätigung der Konformität mit der DSGVO) bedarf es einer Akkreditierung der Zertifizierungsstelle im Sinne von § 39 BDSG in der seit dem 25. Mai 2018 geltenden Fassung anhand der Kriterien, die von der zuständigen Bundes- oder Landesdatenschutzbehörde oder von dem Europäischer Datenschutzausschuss gemäß Art. 63 EU-DSGVO genehmigt worden sind, durch die Deutsche Akkreditierungsstelle (DAkkS). Nähere Informationen hält die DAkkS bereit. Da die DAkkS bislang (Stand: September 2018) noch keine privaten Zertifizierungsstellen akkreditiert hat, gibt es aktuell am Markt noch keine Konformitätsbewertungsaussagen (Zertifikate), die eine Konformität mit den Anforderungen der EU-DSGVO bestätigen.

BMWi – Trusted Cloud

- Projekt des BMWi für Datenschutz und eine Zertifizierung „Projekt Trusted Cloud Datenschutzprofil (TCDP)“. TCDP beschäftigt sich mit der Datensicherheit in Cloud-Diensten und unterstützt Entwicklungen zur sicheren Datenverarbeitung in der Cloud. TCDP ist der Prüfstandard für die Datenschutz-Zertifizierung. Er liegt aktuell als „Kriterienkatalog“ in einer Version 2.0 vor, der am 30.5.2018 veröffentlicht wurde.
- Stiftung Datenschutz (**vor** DSVO): *„Anbieter von Cloud-Diensten können sich nach diesem Standard zertifizieren lassen – der Cloud-Nutzer hat dann seine Kontrollpflicht erfüllt.“*
- BMWI (**heute**): Im Rahmen der Trusted Cloud Plattform wird die Datenschutzzertifizierung für Cloud-Anwendungen aktuell **weiter vorangetrieben**. Derzeit ist die datenschutzkonforme Speicherung und Verarbeitung von Daten ein großes Hindernis bei der praktischen Anwendung. Durch das Zertifikat wird eine datenschutzkonforme und wirtschaftliche Verarbeitung von Daten in und für die Cloud ermöglicht. Damit werden gleichzeitig auch die Voraussetzungen für die Zertifizierung nach der EU-Datenschutz-Grundverordnung geschaffen.

BMWi Projekt Auditor

- Projekt Auditor

Heute (6.6.2018) wird im Bundesministerium für Wirtschaft und Energie (BMWi) ein Kriterienkatalog für die Datenschutzzertifizierung von Cloud-Diensten präsentiert. Die Kriterien sind ein Meilenstein des BMWi-Forschungsprojekts AUDITOR, in dessen Rahmen eine europaweit anerkannte Zertifizierung von Cloud-Diensten nach Maßgabe der EU-Datenschutz-Grundverordnung entwickelt und erprobt wird. Im Zentrum der Zertifizierung steht der Schutz personenbezogener Daten in der Cloud. Sie soll Anbietern, Kunden und Endverbrauchern gleichermaßen Sicherheit geben und die einfache Nutzung von Cloud-Diensten ermöglichen.Das Forschungsprojekt European Cloud Service Protection Certification (AUDITOR) soll 2019 mit ersten Pilotzertifizierungen abgeschlossen werden.

AWS: Vertragskonstruktion

- Kostenlose Accounts, AWS AGB
- Großkunden: Enterprise Customer Agreement
- Affiliate Addendum
- Data Processing Addendum (DPA Stand Mai 2018)
- Annex 1: AWS Security standards
- Annex 2: Standard Contractual Clauses

DPA – Problempunkte (exemplarisch)

- Übermittlung an staatliche Stellen

Confidentiality of Customer Data. AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer.

DPA – Problempunkte (exemplarisch)

- Datenzugriffe AWS Mitarbeiter

Confidentiality Obligations of AWS Personnel. AWS restricts its personnel from processing Customer Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

DPA – Problempunkte (exemplarisch)

- Subunternehmer

Authorised Sub-processors. Customer agrees that AWS may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. The AWS website (currently posted at https://aws.amazon.com/compliance/sub-processors/) lists sub-processors that are currently engaged by AWS to carry out processing activities on Customer Data on behalf of Customer. At least **30 days** before AWS engages any new sub-processor to carry out processing activities on Customer Data on behalf of Customer, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer objects to a new sub-processor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, **Customer may move** the relevant Customer Data to another AWS Region where the new sub-processor to whom Customer objects, is not engaged by AWS as a sub-processor. Customer consents to AWS's use of sub-processors as described in this Section.

DPA – Problempunkte (exemplarisch)

- Sicherheitsvorfälle

Security Incident. AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

Unsuccessful Security Incidents. Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents;

DPA – Problempunkte (exemplarisch)

- Audits

Audit Reports. At Customer's written request, and in place, AWS will provide Customer with a copy - **provided that the parties have an applicable NDA -** of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.

Customer Audits. Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. **If AWS declines** to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement.

Problempunkte: Auswirkungen

- Übermittlung an staatliche Stellen: AWS unterliegt als US-Unternehmen der Kontrolle z.B. des DHS und muss auf Anforderung Daten übermitteln. Es ist nicht sicher, dass der Kunde informiert wird.
- Datenzugriffe Mitarbeiter: was nicht offengelegt wird: die sogenannten Applikationsverantwortlichen haben weltweit Zugriff auf ihre Applikation und können den Bastion-Host umgehen.
- Sicherheitsvorfälle: es scheint nicht garantiert, dass der Kunde seiner Verpflichtung nach Art. 33 DSGVO nachkommen kann. Für KRITIS-Unternehmen problematisch, dass erfolglose Versuche nicht einmal reportet werden.
- Audits: Im Ergebnis kein Anspruch auf eigene Audits. Das Auditrecht wird dadurch ausgeübt, dass AWS Zertifizierungen aufrechterhält. AWS kann einen Auditwunsch ablehnen, dann besteht nur ein Kündigungsrecht.
- Subunternehmer: AWS kann diese beliebig einschalten. Der Auftraggeber wird nicht informiert und muss sich selbst informiert halten. Er kann dem Subunternehmer nicht widersprechen, er kann nur die Daten verlagern, was in der Praxis auf eine Kündigung hinausläuft.
- Audit Subunternehmer: dies ist für den Auftraggeber nicht möglich.

Ergebnis

- Wesentliche Anforderungen der DSGVO werden nicht erfüllt.
- Die OH Cloud Computing wird in mehreren Punkten missachtet.
- Die Zertifikate erfüllen (noch) nicht die Anforderungen der DSGVO.
- Die Verantwortungsmatrix verlagert die Verantwortung des AVV teilweise zurück auf den Kunden.
- Die Haftung von AWS ergibt sich aus dem „Customer Agreement“ und ist limitiert.

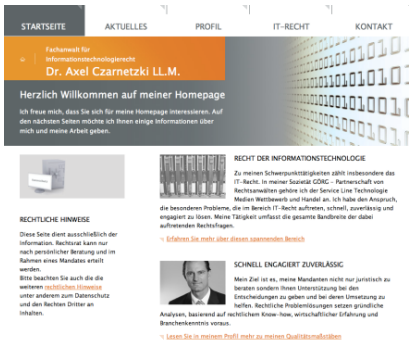
Das bedeutet? Ausblick

- Der Einsatz von AWS für sensible personenbezogene Daten erscheint nicht zulässig, es sei denn, man folgt der Auffassung, dass die Verschlüsselung den Personenbezug aufhebt.
- Objektiv ist die Sicherheitslage bei AWS sehr hoch.
- Bei Anwendung der HomeCloud on AWS on DX dürfte eine Entschlüsselung faktisch ausgeschlossen sein.
- Zertifikate könnte in Zukunft ausreichen und etliche Probleme beseitigen, aber nicht alle.
- Für sehr große Kunden ist AWS zu Verhandlungen über Modifikationen bereit - das ist aber sehr mühsam.

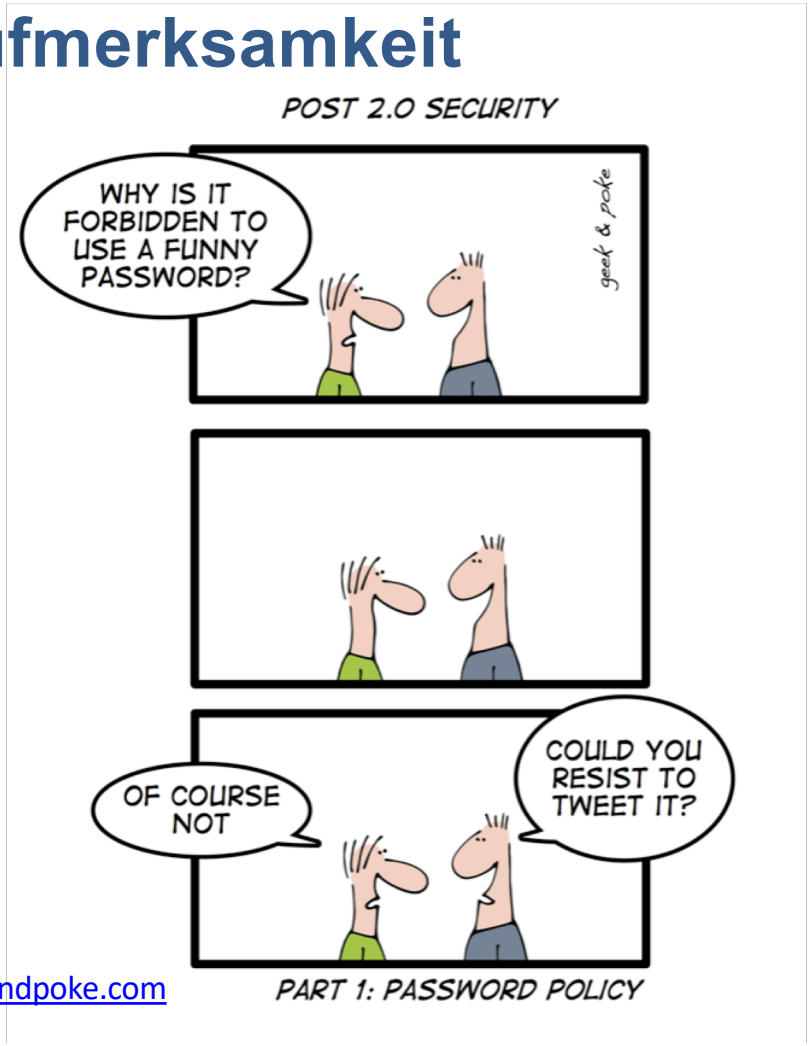
Vielen Dank für Ihre Aufmerksamkeit

GÖRG

www.goerg.de



www.czarnetzki.eu



from geek&poke; Oliver Widder, Hamburg – www.geekandpoke.com