Auslagerung an Cloud-Anbieter

Security und Compliance: Grundlagen und Best Practices für die Public Cloud

Gerald Boyne
Principal Security & Compliance Strategist DACH

Agenda

AWS – FUNDAMENTALS, REGIONEN & ZONEN = ∑ DC

ANFORDERUNGEN DES DATENSCHUTZES = DSGVO

- PRIVACY SHIELD INVALIDIERUNG // SCHREMSII
- DATENSCHUTZ = GETEILTE AUFGABE
- TECHNISCHER DATENSCHUTZ = SUPPLEMENTARY MEASURES
- DATENSCHUTZNACHWEISE = ZERTIFIZIERUNGEN

CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT = CLOUD ACT

AWS@GAIA-X

Q&A

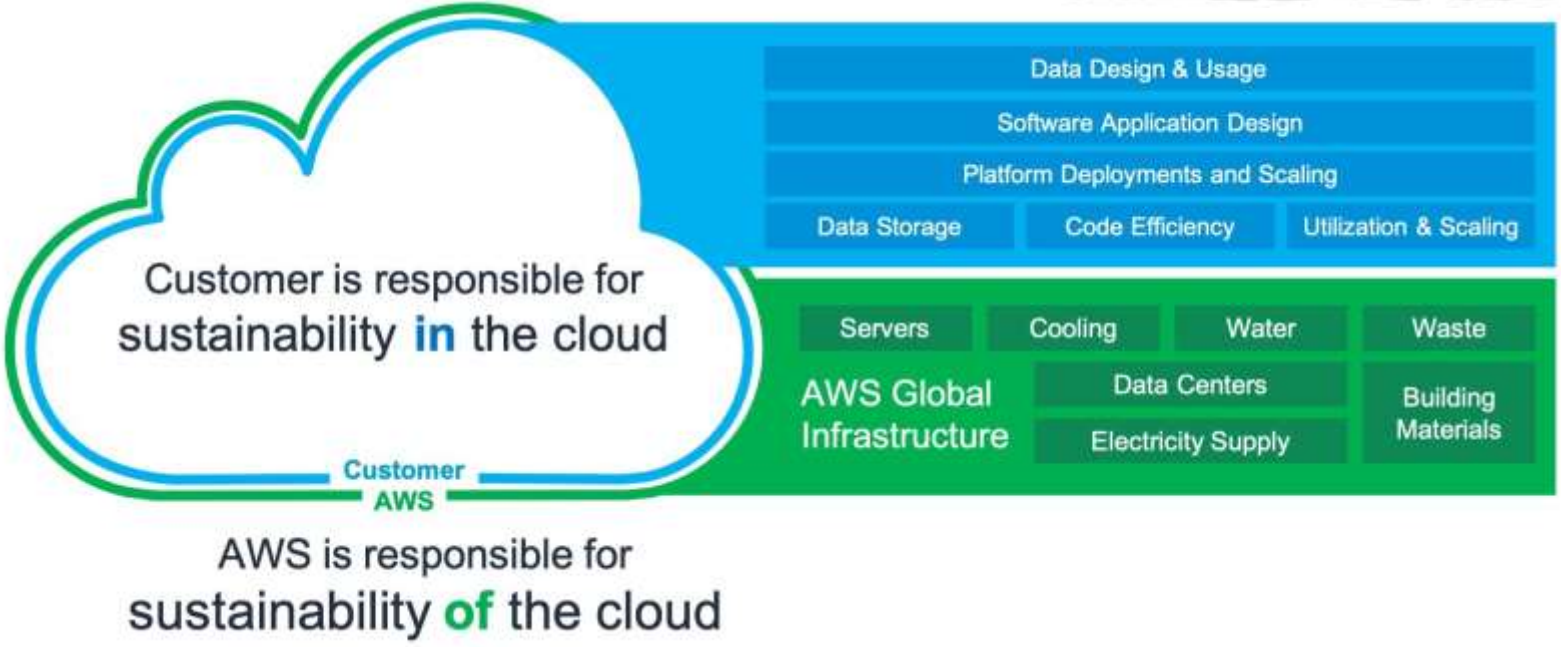
AWS – FUNDAMENTALS
REGIONEN & ZONEN
= ∑ DC

Globales Netzwerk

Stand 23.05.2023

https://aws.amazon.com/de/about-aws/global-infrastructure/

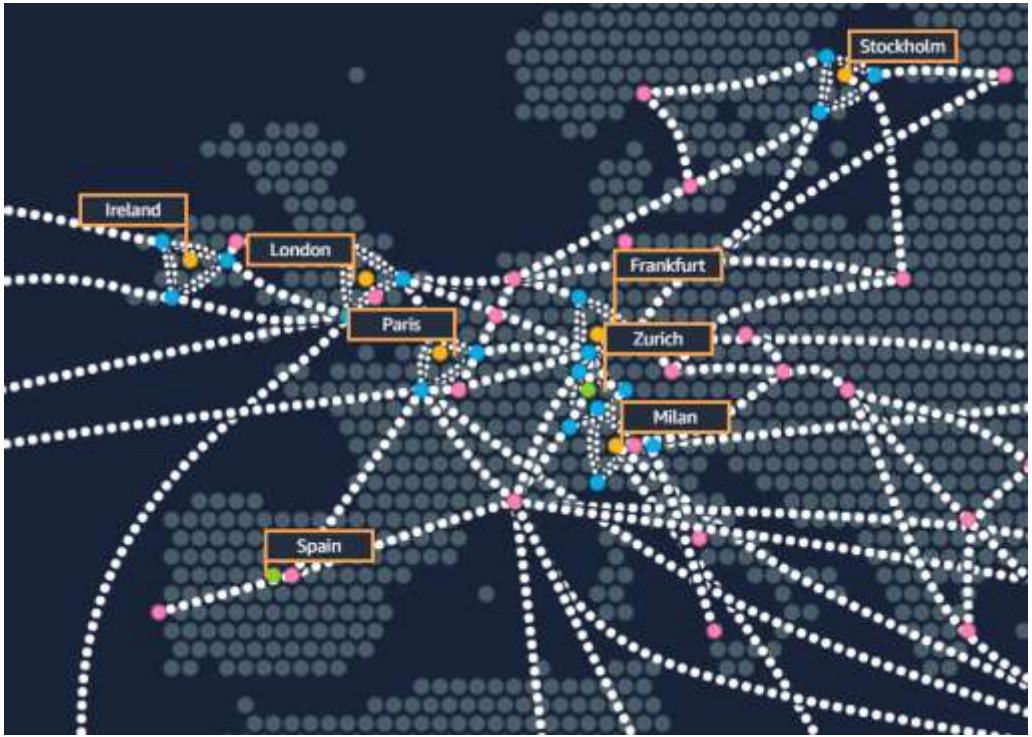
- geht nur gemeinsam

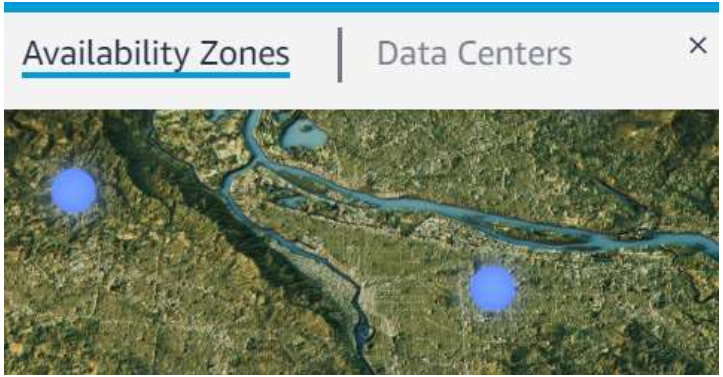


https://aws.amazon.com/de/blogs/aws/new-customer-carbon-footprint-tool/

https://aws.amazon.com/de/blogs/architecture/optimizing-your-aws-infrastructure-for-sustainability-part-i-compute/

Abdeckung in der EU





Eine Availability Zone (AZ) umfasst ein oder mehrere eigene Rechenzentren mit redundanter Stromversorgung und Netzwerkanbindung in einer AWS-Region. **Mithilfe von AZn können Sie Produktionsanwendungen und Datenbanken betreiben, die verfügbarer, fehlertoleranter und skalierbarer sind,** als dies von einem einzigen Rechenzentrum aus möglich wäre. Alle AZn in einer AWS-Region sind über ein Netzwerk aus eigenen, vollständig redundanten Metro-Glasfaserkabeln mit hoher Bandbreite und niedriger Latenz verbunden. Dies ermöglicht einen Datenaustausch mit hohem Durchsatz und niedriger Latenz zwischen den einzelnen AZn. **Der gesamte Datenverkehr zwischen AZn ist verschlüsselt**. Die Netzwerkleistung ist ausreichend, um eine synchrone Replikation zwischen AZn zu erreichen. AZ erleichtern die Partitionierung von Anwendungen für hohe Verfügbarkeit. Wenn die Partition einer Anwendung auf mehrere AZn verteilt ist, ist die Anwendung besser isoliert und vor Ereignissen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben usw. geschützt. AZn sind physisch durch eine hinlängliche Entfernung von jeder anderen AZ getrennt, obwohl alle innerhalb von 100 km voneinander liegen.

https://www.infrastructure.aws/

Einschränkung auf eine Region wie Frankfurt?

12.1 **Regionen**. **Der Kunde kann den/die Standort bestimmen**, an denen die Verarbeitung der Kundendaten innerhalb des AWS-Netzwerks stattfinden soll - jeweils eine „AWS-Region".
Sobald eine Entscheidung des Kunden vorliegt, wird AWS aus der/den gewählten Regionen(en) Kundendaten nur dann in (eine) andere Region(en) übermitteln,
wenn es für die Bereitstellung von Services auf Anfrage des Kunden
oder die Einhaltung gesetzlicher Bestimmungen bzw. verbindlicher Anordnungen staatlicher Stellen erforderlich ist.

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

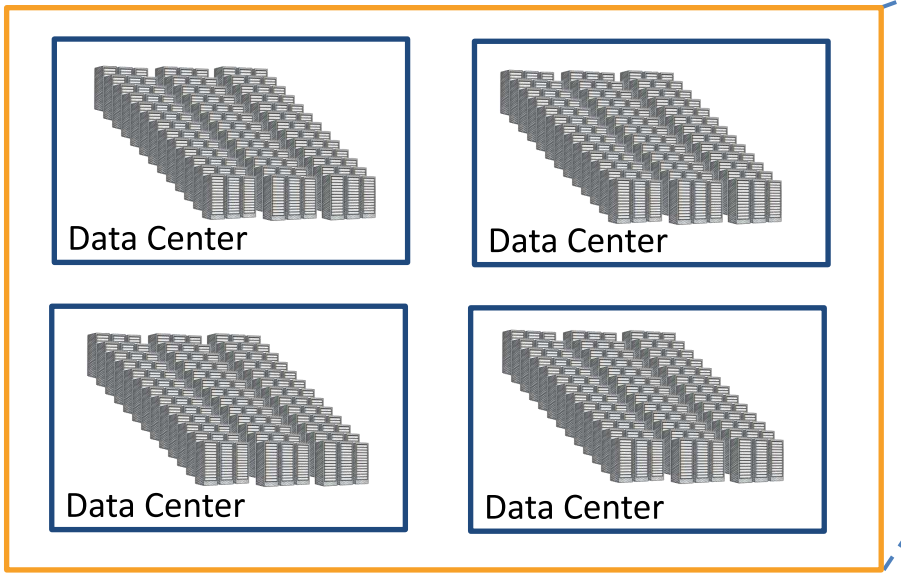
Mit Service- Kontroll-richtlinien (SCPs) kann der Zugriff auf bestimmte AWS-Regionen beschränkt werden
(weitere Konfigurationen notwendig!)

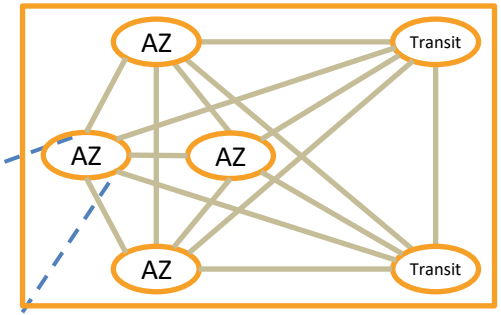

```
{
    "Effect" : "Allow",
    "Action" : "*",
    "Resource" : "*",
    "Condition":
 {
    "StringEquals": {
       "aws:RequestedRegion": "eu-central-1„
                    }
 }
}
```

```
{
    "Sid": "DenyAllOutsideEU",
    "Effect": "Deny",
    "NotAction": [
       "iam:*",
       "organizations:*",
       "route53:*",
       "budgets:*",
       "waf:*",
       "cloudfront:*",
       "globalaccelerator:*",
       "importexport:*",
       "support:*"
    ],
    "Resource": "*",
    "Condition": {
        "StringNotEquals": {
            "aws:RequestedRegion": [
                "eu-central-1",
                "eu-west-1"
            ]
        }
    }
```

https://aws.amazon.com/de/about-aws/whats-new/2019/03/service-control-policies-enable-fine-grained-permission-controls/

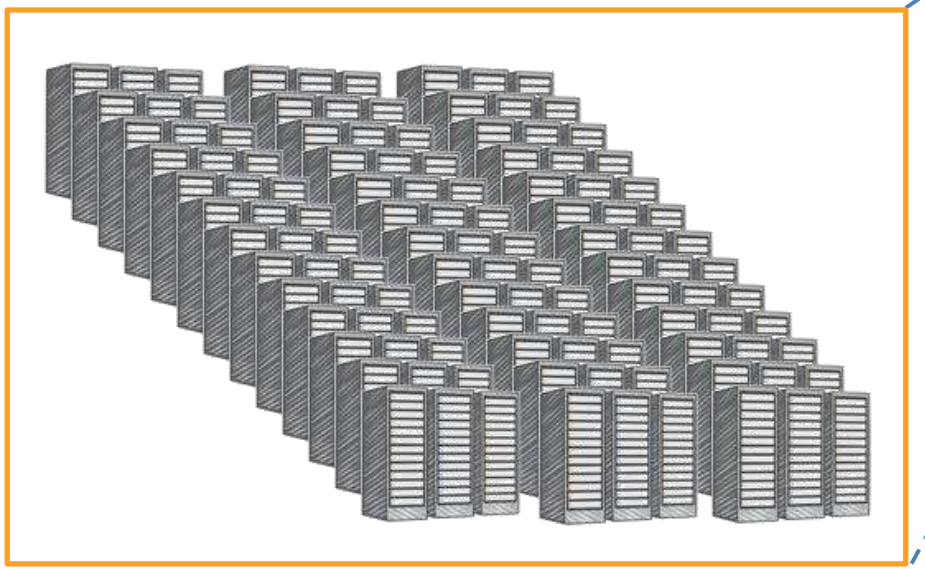
AWS Availability Zone

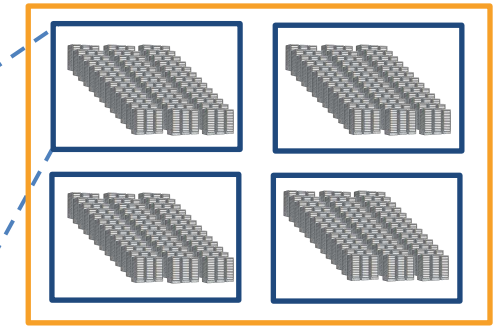




- 1 von 81 AZs weltweit
- Alle Regionen haben 2 oder mehr AZs
- Jeder AZ ist 1 oder mehr DC
  - Kein Rechenzentrum befindet sich in zwei AZs
  - Einige AZs haben bis zu 6 DCs
- DCs in AZ weniger als ¼ ms voneinander entfernt

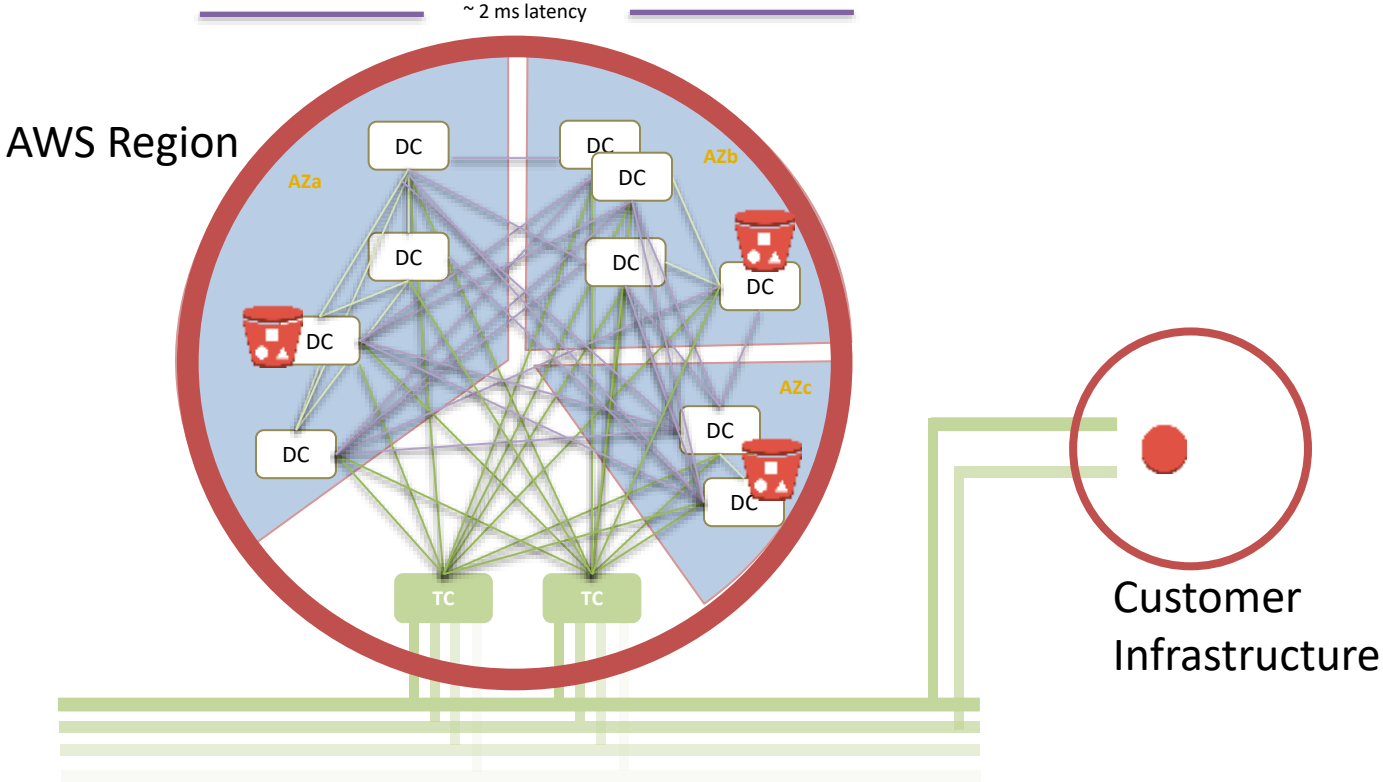
AWS Data Center



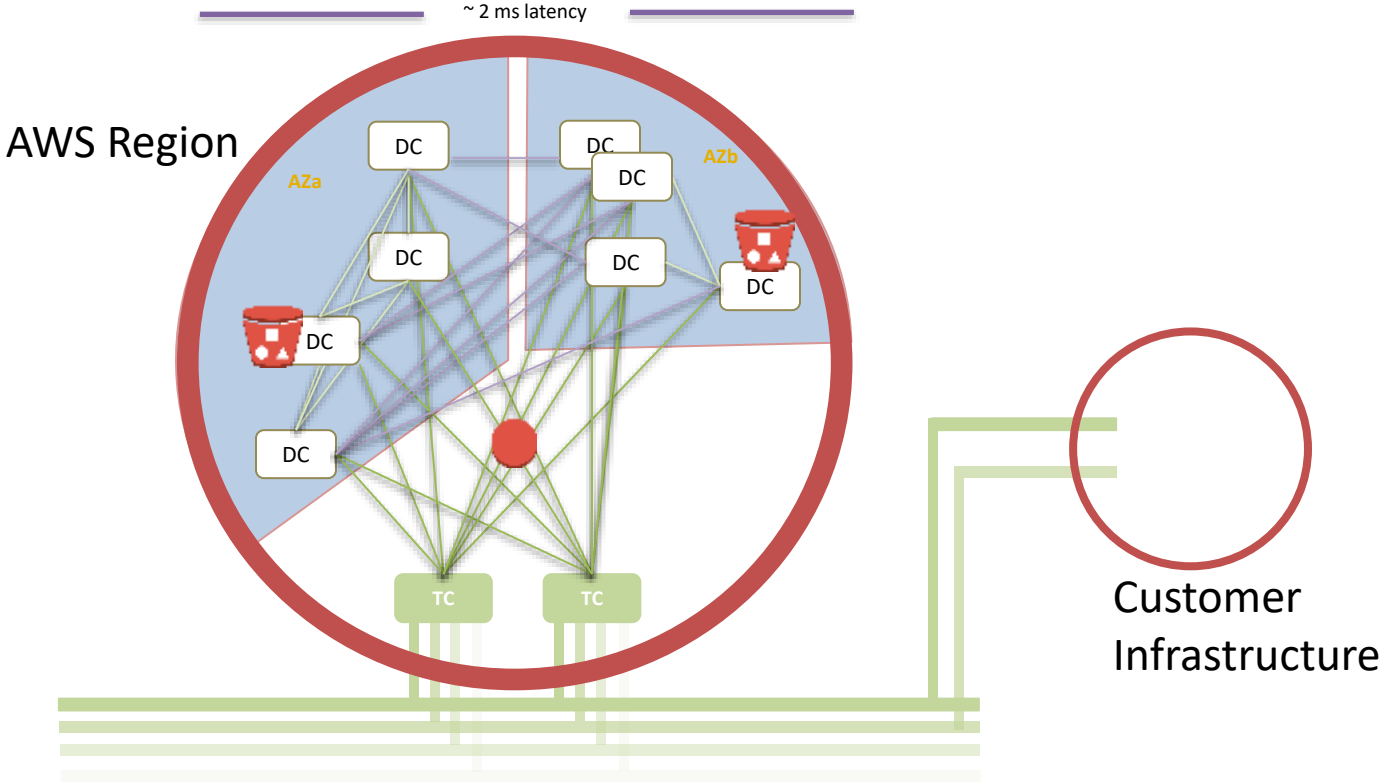


- Einzelne DCs zwischen 25 und 32 MW Leistungsaufnahme
- Größere DCs unerwünscht (Risikominderung)
- Bis zu 102 Tbit/s für einen einzelnen DC bereitgestellt (Inter-DC nicht Intra)

Übersicht

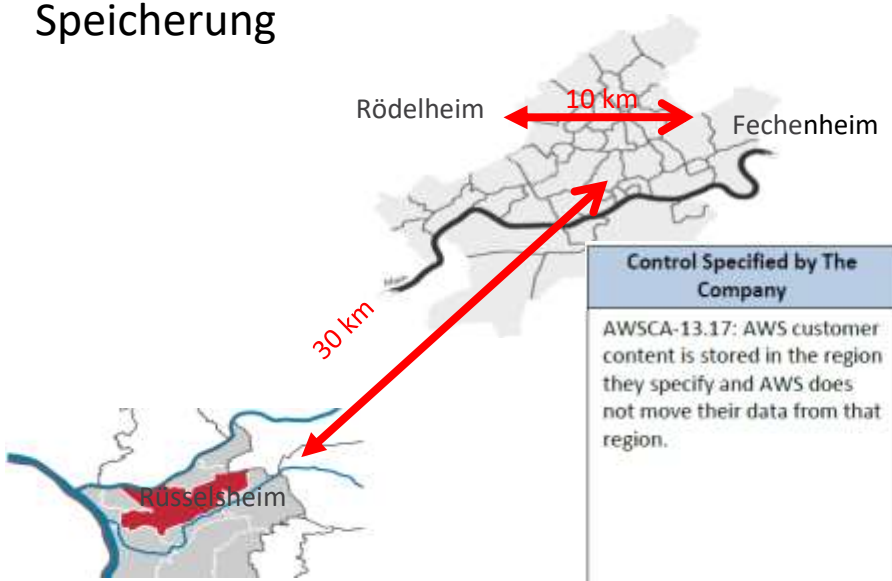


Übersicht



C5- Testierung

- Umfeldparameter
- Souveränität des Kunden bei der Auswahl des Ortes der Verarbeitung und Speicherung



Control Specified by The Company	C5 Requirement	Testing Performed by EY and Results of Tests
AWSCA-13.17: AWS customer content is stored in the region they specify and AWS does not move their data from that region.	AM-08, RB-03, RB-06	Inquired of the AWS Compliance Program Manager and ascertained that cloud customer can choose the region or regions, which he would like to use for the purpose of his data processing and storage including backups in encrypted form that conforms to the current state of the art. **No deviations noted.** Selected a sample of services, created resources in a certain region and ascertained the services are appropriately configured for the respective region. **No deviations noted.**

AWS Artifact

- AWS Artifact bietet On-Demand-Zugriff auf die Sicherheits- und Compliance-Berichte von AWS und ausgewählte Online-Vereinbarungen.
- Die meisten Artefakte stehen allen Kunden ohne weitere Genehmigung zur Verfügung.
- Eine kleine Anzahl von Artefakten erfordert eine zusätzliche Geheimhaltungsvereinbarung (NDA).

Titel	Berichtszeitraum	Kategorie	Beschreibung
C5 Continued Operations Letter	1. Oktober 2020 bis 31. Dezember 2021	Certifications and Attestations	This document states that we continue to maintain the security controls and system environment that was audited and described in the latest C5 report. For information about the services and AWS Regions that this document applies to, see the current AWS C5 report.
Cloud Computing Compliance Controls Catalogue (C5) - (Deutsch/German)	1. Oktober 2018 bis 30. September 2019	Certifications and Attestations	Dieses Dokument bewertet die AWS-Controls, die die Kriterien des Cloud Computing Compliance Controls Catalog (C5) erfüllen, der vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt wurde.
Cloud Computing Compliance Controls Catalogue (C5) - Current	1. Oktober 2019 bis 30. September 2020	Certifications and Attestations	This is the most recent AWS C5 Report. This document evaluates the AWS controls that meet the criteria developed by the German BSI (National Security Authority) for Cloud Computing Compliance Controls Catalog (C5).
Cloud Computing Compliance Controls Catalogue (C5) - Previous	1. Oktober 2018 bis 30. September 2019	Certifications and Attestations	This is the AWS C5 Report for the period of October 1, 2017 to September 30, 2018. This document evaluates the AWS controls that meet the criteria developed by the German BSI (National Security Authority) for Cloud Computing Compliance Controls Catalog (C5).

https://console.aws.amazon.com/artifact

ANFORDERUNGEN DES DATENSCHUTZES = DSGVO

Definition von Souveränität bei IT Verfahren

Das Ausmaß zu dem Staatsgewalten, legitim Zugang zu extraterritorial gespeicherten Daten erhalten können

Die Reichweite von fremden Geheimdiensten und anderen Überwachungsorganen, Zugang zu Daten zu erhalten, nachdem diese übertragen worden sind

Daten Souveränität

Unser Ziel ist es,

die Souveränität von Daten in allen AWS services in den bestehenden, kommerziellen Regionen zu erfüllen,

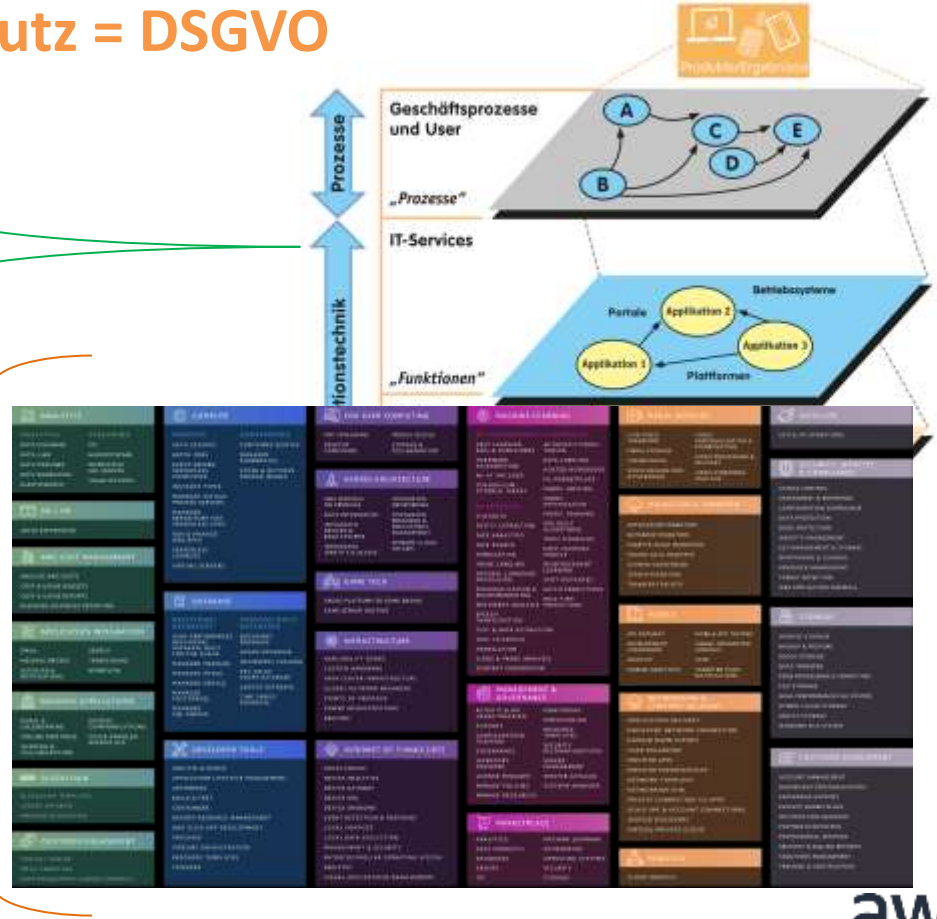
indem wir unsere technischen Möglichkeiten, lesbare Informationen zu extrahieren komplett eliminieren.

https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/

Anforderungen von Datenschutz = DSGVO

Die Sieben Grundprinzipien der DSGVO

- Legitimität
- Einschränkung des Zwecks
- Daten-Minimierung
- Korrektheit
- Speicherdauerbegrezung
- **Integrität & Vertraulichkeit**



TOMs des Verantwortlichen vs. des Auftragsverarbeiters

Verantwortlicher

Zugriffskontrolle | Protokollierung |IDS / IPS …

Um das Verfahren und somit die personenbezogenen Daten zu schützen

Auftragsverarbeiter

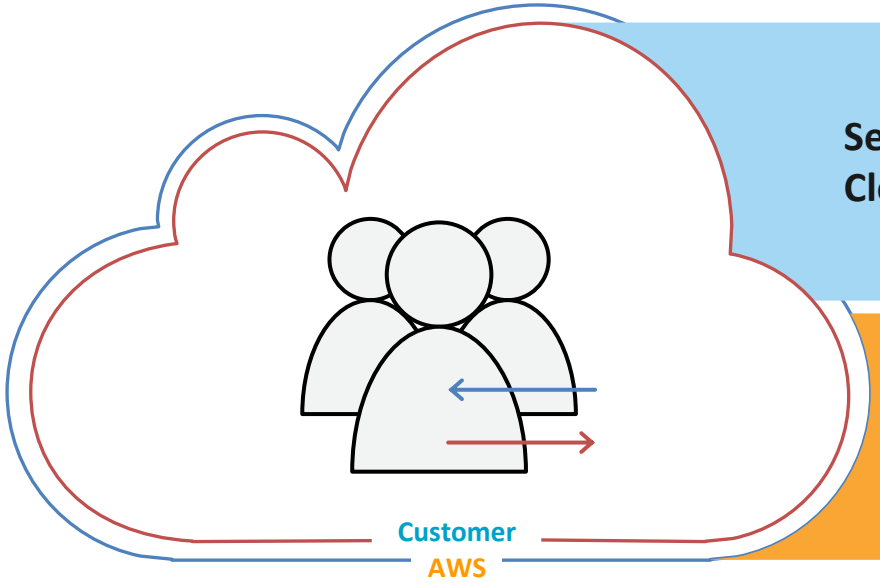
Zugriffskontrolle | Protokollierung |IDS / IPS …

um die Cloud zu schützen

Und somit die Virt… Private Cloud (VPC) des Kunden

DATENSCHUTZ
GETEILTE AUFGABE

Modell der geteilten Verantwortung



Security IN der Cloud

Der Kunde verantwortet die richtige Nutzung der AWS Services, sowie den sicheren und korrekten Umgang mit den Daten in seiner **Anwendung**

Security DER Cloud

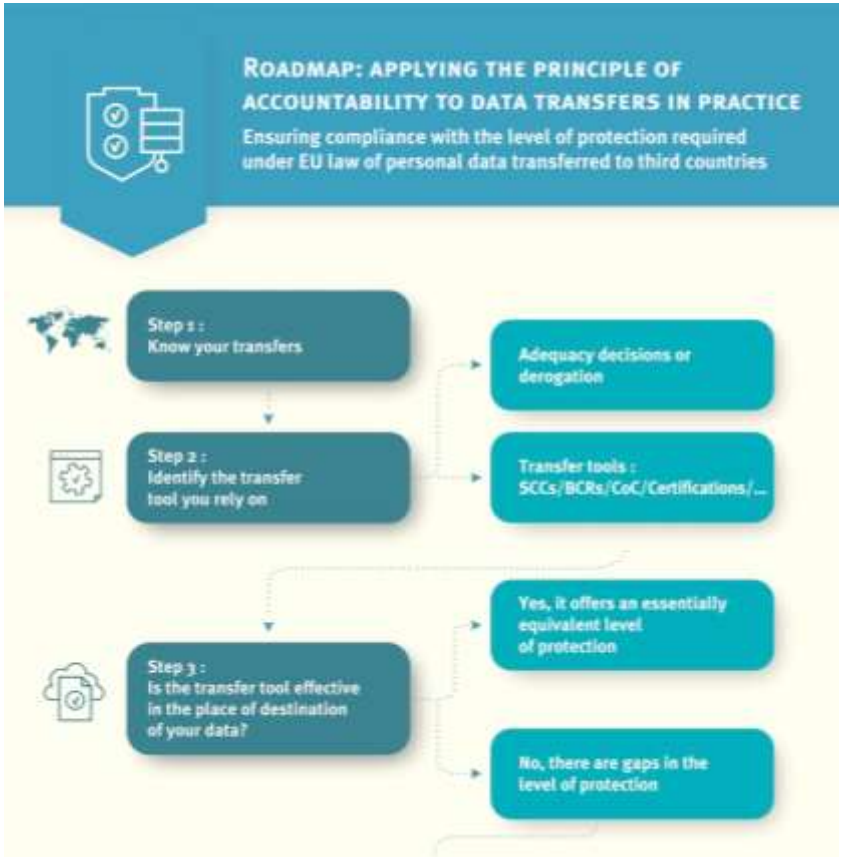
AWS verantwortet den Schutz der Infrastruktur, sowie die korrekte Funktion der AWS Services – also der **Cloud**

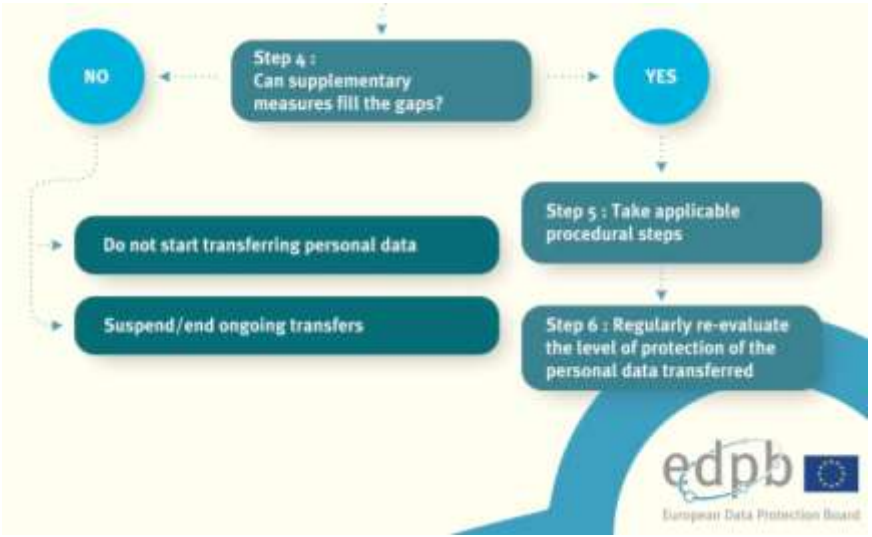
EU-Zertifizierungsschemas für **Cloud-Dienste**

Dazu sagte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Professor Ulrich Kelber:
„Die Nutzung von Cloud-Diensten ist im Alltag praktisch, aber es muss eben auch sicher sein. Ein EU-Zertifizierungsschema kann den Bürgerinnen und Bürgern dabei helfen, die Sicherheit von Cloud-Diensten besser zu bewerten. Es würde mich freuen, wenn sich darin wesentliche Teile des C5-Kriterienkatalogs wiederfinden.
Wichtige Teilaspekte des Datenschutzes würden so direkt mit berücksichtigt.“

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210127_C5_Datenschutz.html

privacy shield – JA – NEIN - aber





https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
https://www.engage.hoganlovells.com/knowledgeservices/news/edpb-issues-comprehensive-schrems-ii-guidance-including-recommended-supplemental-measures-to-protect-international-data-transfers

privacy shield – JA – NEIN - aber

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder **bewertet Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern** auf personenbezogene Daten, die nach Art. 28 DSGVO im Auftrag im EWR verarbeitet werden, datenschutzrechtlich wie folgt:

1. **Die Gefahr allein**, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, **genügt nicht, um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO anzunehmen.**

2. Allerdings kann eine solche Gefahr dazu führen, dass solchen Rechtsvorschriften unterliegenden Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, **soweit nicht diese – oder auch der Verantwortliche – technische und/oder organisatorische Maßnahmen ergriffen haben, die hinreichend Garantien dafür bieten**, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen angeht, **im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.**

https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf

privacy shield – JA – NEIN - aber

3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass personenbezogene Daten in Drittländer ohne einen Angemessenheitsbeschluss nur dann übermittelt werden dürfen, wenn hierfür geeignete Garantien vorgesehen sind. Diese Garantien können beispielsweise in genehmigten Verhaltensregeln oder Zertifizierungsmechanismen als Transferinstrumente für Drittstaatentransfers bestehen.


Guidelines 07/2022 on certification as a tool for transfers

Version 1.0

Adopted on 14 June 2022

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en

Hierzu hat der Europäische Datenschutzausschuss (EDSA auf Basis der Vorarbeiten der Expert Subgroup International Transfers (ITS ESG) zwei entsprechende Leitlinien angenommen.

Zum einen handelt es sich um die Leitlinien für Zertifizierungen (Guidelines 07/2022 on certification as tool for transfers)und zum anderen um die für genehmigte Verhaltensregeln (Guidelines 04/2021 on codes of conduct as tools for transfers).

Damit hat der EDSA jetzt zu allen Transferinstrumenten („geeignete Garantien“ im Sinne des Art. 46 DSGVO) veröffentlicht.

Guidelines 07/2022 on certification as tool for transfers , abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.pdf

Datenschutz

Anwendungsfall 1: Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern

Ein Datenexporteur nutzt einen Hosting-Anbieter in einem Drittland zur Speicherung personenbezogener Daten, z. B. für Backup-Zwecke. Wenn :

1. die personenbezogenen Daten vor der Übermittlung mit einer dem Stand der Technik entsprechenden, starken Verschlüsselungsmethode verschlüsselt werden;
2. der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. ggf. Schlüssellänge, Betriebsmodus) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute- Force-Angriffe) – Robustheit gegen die von den Behörden im Empfängerland durchgeführte Kryptoanalyse bieten;
3. die Verschlüsselungsstärke den spezifischen Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;
4. der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus z. B. durch Zertifizierung bestätigt wurde;
5. die Schlüssel zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden und
6. die Konformität die Schlüssel allein beim Datenexporteur oder bei anderen mit dieser Aufgabe betrauten Stellen im EWR oder in einem Drittland, in einem Gebiet oder in einem oder mehreren Sektoren eines Drittlands oder einer internationalen Organisation liegt, wobei die Kommission durch einen Angemessenheitsbeschluss gemäß Artikel 45 DSGVO festgestellt hat, dass dort ein angemessenes Schutzniveau gewährleistet ist;

stellt die vorgenommene Verschlüsselung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

Betreiberausschluss

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

Datenschutz

Anwendungsfall 6: Übermittlung an Cloud-Service-Anbieter oder andere Verarbeiter, die Zugang zu unverschlüsselten Daten benötigen

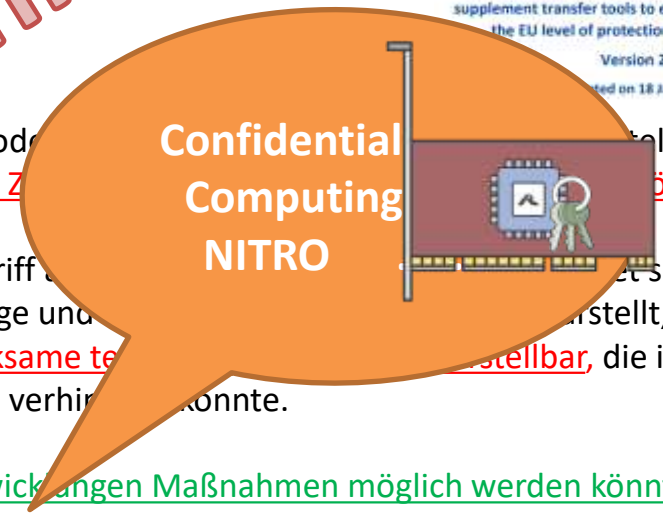
Ein Datenexporteur beauftragt einen Cloud-Service-Anbieter oder anderen Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten, die im Drittland nach den Anweisungen des Datenexporteurs erfolgt.
Wenn:

1. ein Verantwortlicher Daten an einen Cloud-Service-Anbieter oder [illegible]lt;
2. der Cloud-Service-Anbieter oder sonstige Auftragsverarbeiter Z[illegible]ötigt, um die ihm übertragene Aufgabe auszufü[illegible]r und
3. die Behörden im Empfängerland Befugnissen für den Zugriff [illegible]t sind, die über das, was in einer demokratischen Gesellschaft eine notwendige und [illegible]rstellt, hinausgehen

ist für den EDSA nach dem derzeitigen Stand der Technik keine wirksame te[illegible]stellbar, die im Falle eines solchen Zugangs die Verletzung der Rechte betroffener Personen verhin[illegible]könnte.

Der EDSA schließt nicht aus, dass durch künftige technische Entwicklungen Maßnahmen möglich werden könnten, die die beabsichtigten Geschäftszwecke erfüllen, ohne dass Zugang zu den unverschlüsselten Daten benötigt würde.


Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Version 2.0
[illegible]ted on 18 June 2021



Betreiberausschluss

https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

privacy shield — JA — NEIN — aber

Regional oder global

Sie können auf die unterstrichenen Häkchen in der folgenden Tabelle klicken, um die AWS-Dokumentation darüber anzuzeigen, wie die AWS-Services Kunden das Verschlüsseln, Löschen und Überwachen der Verarbeitung ihrer Kundendaten ermöglichen.

AWS-Service	Kunde kann verschlüsseln	Kunde kann löschen	Kunde kann die Verarbeitung überwachen	Kein Fernzugriff*
Alexa for Business	✓	✓	✓	✓
Amazon API Gateway	✓	✓	✓	✓
Amazon AppFlow	✓	✓	✓	✓

Liste anzeigen »

*Es sei denn, der Zugriff wird von ihnen angefordert, oder ist zur Verhinderung von Betrug und Missbrauch oder zur Einhaltung von Gesetzen erforderlich.

AWS-Services, die es Kunden ermöglichen, die Übermittlung von Kundendaten zu deaktivieren

Die folgenden AWS-Services übermitteln Kundendaten, um diese Services zu entwickeln und zu verbessern, und Sie können diese Übermittlung deaktivieren.

- Amazon CodeGuru Profiler
- Amazon Comprehend
- Amazon Connect Customer Profiles for Identity Resolution

Liste anzeigen »

AWS-Services, die Kundendaten als wesentliche Funktion des Services übermitteln

Die folgenden AWS-Services übermitteln Kundendaten als wesentliche Funktion des Services. Wenn Sie sich beispielsweise entschließen, Nachrichten über den Amazon-Simple-Notification-Service zu senden, wird der Inhalt dieser Nachrichten an den Standort der Empfänger übermittelt.

- Alexa for Business
- Amazon AppStream 2.0 Benutzerpool

Liste anzeigen »

https://aws.amazon.com/de/compliance/privacy-features/

privacy shield — JA — NEIN — aber

Regional oder global

AWS-Services, die Kundendaten als wesentliche Funktion des Services übermitteln

Die folgenden AWS-Services übermitteln Kundendaten als wesentliche Funktion des Services. Wenn Sie sich beispielsweise entschließen, Nachrichten über den Amazon-Simple-Notification-Service zu senden, wird der Inhalt dieser Nachrichten an den Standort der Empfänger übermittelt.

- Alexa for Business
- Amazon AppStream 2.0 Benutzerpool
- Amazon Chime
- Amazon CloudFront
- AWS Elemental MediaConnect
- Amazon Pinpoint
- Amazon Simple Email Service
- Amazon Simple Notification Service

https://aws.amazon.com/de/compliance/privacy-features/

privacy shield — JA — NEIN — aber ☺

Was kann ein AWS-Kunde tun?

1. Wählen Sie AWS-Services aus, die im **EU-Raum** angeboten werden
   => kein Datenexport in die USA

2. **Verschlüsseln** der Daten (mit persönlichem Bezug) at rest
   => zusätzliche Schutzmaßnahmen
3. **Verschlüsseln** des gesamten eigenen Netzwerkverkehrs in transit
   => zusätzliche Schutzmaßnahmen
4. **Confidential Computing** für die Datenverarbeitung in process
   => zusätzliche Schutzmaßnahmen

5. **Beschränken Sie Supportfälle nur auf die Testumgebung**
   => kein Datenexport in die USA

6. Prüfen der Implementierung gemäß des **WellArchitected Frameworks** (best practices)
   => zusätzliche Schutzmaßnahmen

7. Aufbau eines **Datenschutzkonzeptes mit TOM** zur Verwendung von AWS
   => Überblick über die getroffenen Schutzmaßnahmen

TOM = Technische und Organisatorische Maßnahmen

Pseudonymisierung / Anonymisierung

Abb. 1: Pseudonymisierung und Anonymisierung von Daten

https://www.johner-institut.de/blog/medizinische-informatik/anonymisierung-und-pseudonymisierung/

Pseudonymisierung / Anonymisierung

Das Datenschutzrecht ermöglicht dabei keineswegs nur die Verarbeitung anonymer Daten, die ganz ohne Personenbezug auskommen.
Namentlich Verschlüsselung und Pseudonymisierung von Personendaten dienen als **„Ermöglichungswerkzeuge“** zur technischen Absicherung des Schutzes bei der Verarbeitung auch großer Datenmeng .

Es existieren verschiedene Ansätze einer Anonymisierung.
• Ist der Personenbezug praktisch für jedermann unmöglich, spricht man von absoluter Anonymisierung
• Die faktische bzw. relative Anonymisierung zeichnet sich dadurch aus, dass die Re-Identifizierbarkeit der betroffenen Person nicht gänzlich ausgeschlossen ist. Allerdings scheidet eine Re-Identifizierung der betroffenen Person aufgrund der Unverhältnismäßigkeit ihres Aufwandes aus.

https://stiftungdatenschutz.org/praxisthemen/anonymisierung#c3502

Pseudonymisierung / Anonymisierung

3.3.3 Gesonderte Aufbewahrung der zusätzlichen Informationen

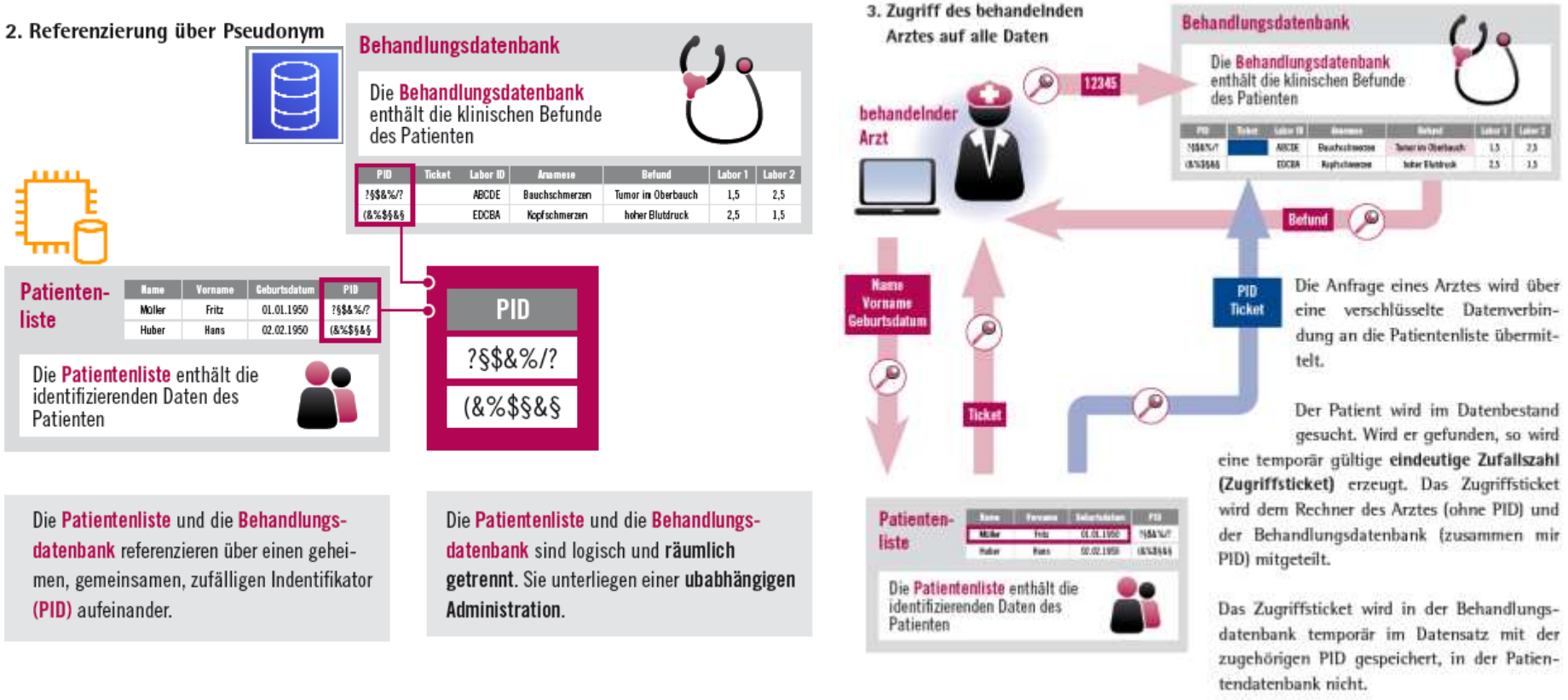
Pseudonymisierte Daten und vorhandene zusätzliche Informationen, die eine Re-Identifizierung eines Betroffenen ermöglichen, müssen **getrennt verarbeitet werden**. Werden personenbezogene Klartextdaten bspw. mittels kryptographischer Verfahren pseudonymisiert, hat die verantwortliche Stelle dafür zu sorgen, dass der kryptographische Schlüssel zur zum Wiederherstellen des Personenbezugs gesondert aufbewahrt wird.

Eine solche Trennung kann auf **logischer Ebene** (z.B. durch Berechtigungskonzepte) aber auch auf **physikalischer Ebene** (z.B. mittels dezidierter Datenverarbeitungs-anlagen) oder **organisatorischer Ebene** (z.B. über einen Datentreuhänder) erfolgen.

Eine Aufteilung auf mehrere Verantwortliche wird vom Gesetzeswortlaut nicht gefordert.

https://stiftungdatenschutz.org/praxisthemen/anonymisierung#c3502

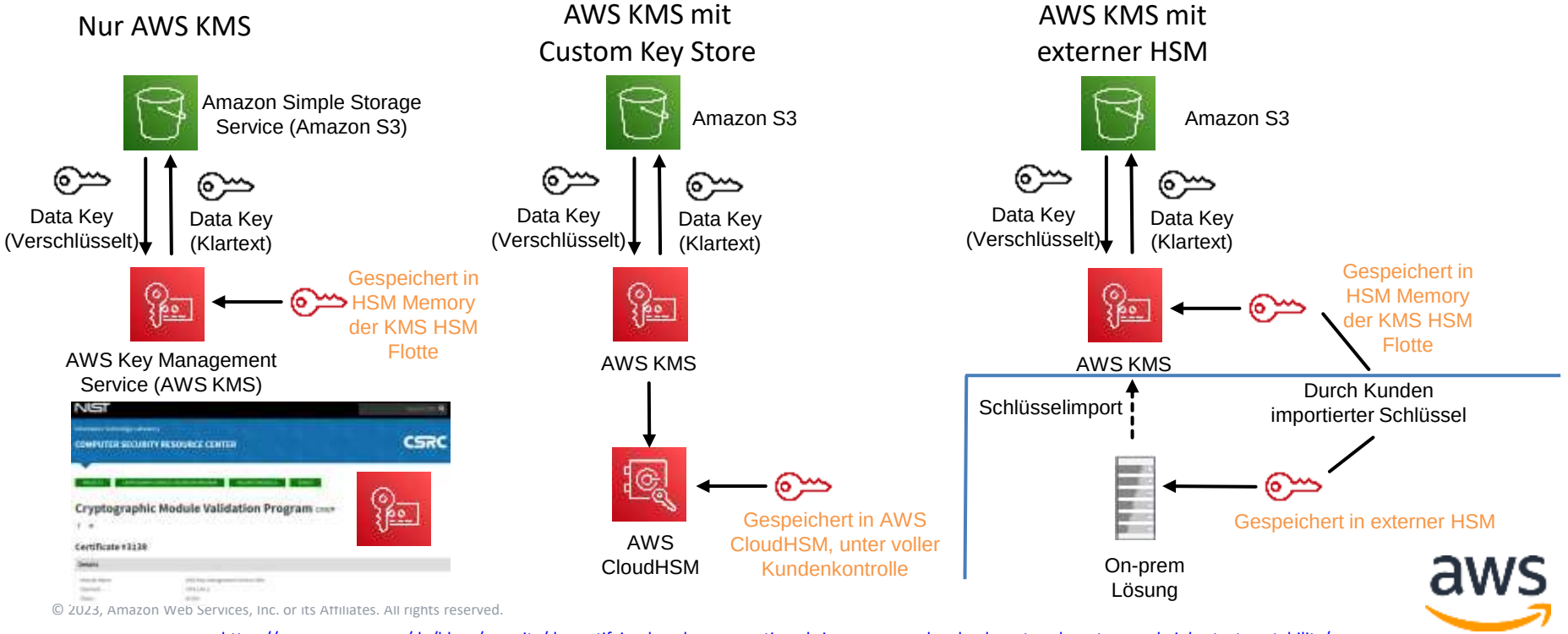
Beispiel durch eine geeignete Referenzierung in getrenntem System



https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung

Crypto@AWS wo liegen die CMK? Wer verwaltet diese?

AWS Optionen für das Schlüsselmanagement in der Cloud – am Beispiel von AWS S3 SSE-KMS



https://aws.amazon.com/de/blogs/security/demystifying-kms-keys-operations-bring-your-own-key-byok-custom-key-store-and-ciphertext-portability/

Confidential Computing NITRO

Das **AWS Nitro-System** bietet drei Haupttypen von Schutz:

1. Schutz vor Cloud-Betreibern

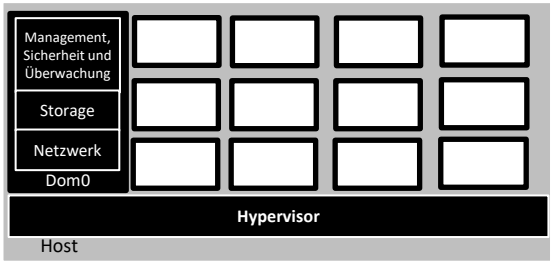
2. Schutz vor AWS-Systemsoftware

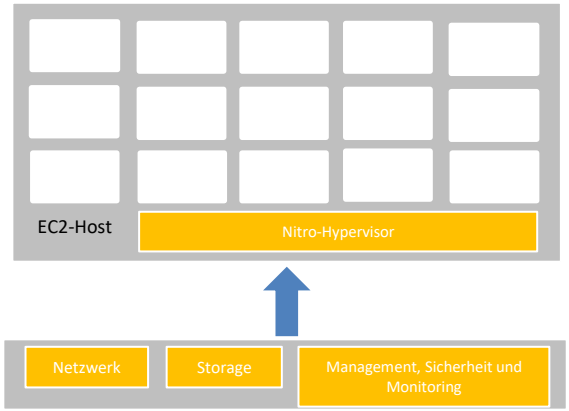
3. Schutz vor eigenen Betreibern und Software des Kunden (Enclave)

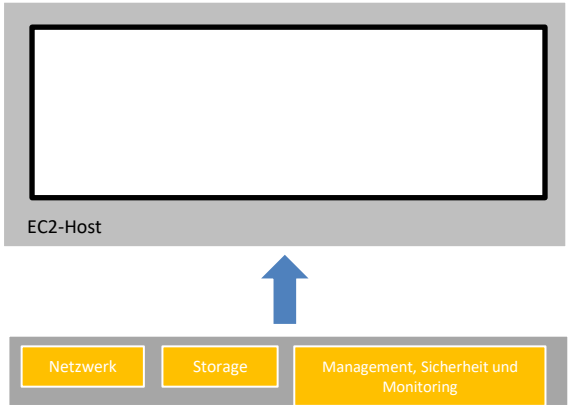
- Das Sicherheitsmodell von **AWS Nitro** System ist gesperrt und verbietet den administrativen Zugriff, wodurch die Möglichkeit menschlicher Fehler und Manipulationen ausgeschlossen werden.

https://aws.amazon.com/de/ec2/nitro

Virtualisierung für die Cloud neu erfunden







Klassische Virtualisierung

- Große Trusted Computing Base (TCB) mit Netzwerk, Speicher und Überwachung werden alle auf derselben Hardware ausgeführt, auf der die VMs der Kunden ausgeführt werden
- Reduziert die Leistung und Ressourcen für VMs

AWS Nitro-System

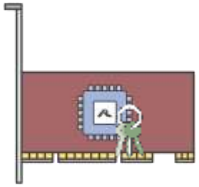
- TCB deutlich reduziert
- Virtualisierung von Netzwerk und Speicher sowie Monitoring laufen auf separater, isolierter, gesicherter Hardware
- Verbietet jeglichen administrativen Zugriff, einschließlich derjenigen von Amazon-Mitarbeitern
- Nur ein dünner Hypervisor auf dem Host

EC2 Bare-Metal-Instanzen

- Alle Funktionen von EC2 und Vorteile von Nitro, aber ohne Hypervisor
- Kunden können Anwendungen bereitstellen, die physische Hardware-Ressourcen verwenden, direkt in der AWS-Infrastruktur
- Nota bene: mac1.metal

https://aws.amazon.com/de/blogs/security/confidential-computing-an-aws-perspective/

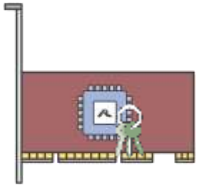
Confidential computing: der AWS Ansatz - NITRO



- Wir haben das Nitro-System so konzipiert, dass es keinen Bedienerzugriff mehr gibt.
- Mit dem Nitro-System gibt es keinen Mechanismus für ein System oder eine Person, um sich bei EC2-Servern (der zugrunde liegenden Host-Infrastruktur) anzumelden oder den Speicher von EC2-Instances zu lesen oder auf Daten zuzugreifen, die im Instance-Speicher und verschlüsselten EBS-Volumes gespeichert sind.
- Wenn ein AWS-Mitarbeiter, einschließlich derjenigen mit den höchsten Berechtigungen, Wartungsarbeiten am EC2-Server durchführen muss, kann er nur mit einem streng begrenzten Satz authentifizierter, autorisierter und geprüfter Verwaltungs-APIs arbeiten.
- Keine dieser APIs kann auf Kundendaten auf dem EC2-Server zugreifen.
- Da diese technologischen Beschränkungen in Nitro System selbst eingebaut sind, kann kein AWS-Administrator diese Kontrollen und Schutzmaßnahmen umgehen.

https://aws.amazon.com/de/blogs/security/confidential-computing-an-aws-perspective/

DRAM encryption @ NITRO



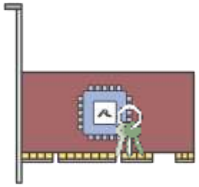
Heute ist die Arbeitsspeicherverschlüsselung per default aktiviert bei:

- **Arm-based** Graviton2-based instances
- **Intel-based** M6i instances, mit Total Memory Encryption (TME)

- Zukünftige EC2 Instanztypen die auf dem **AMD Milan processor** aufbauen nutzen Secure Memory Encryption (SME)

https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/

AMD SEV-SN @ NITRO



AMD SEV-SNP = Secure Encrypted Virtualization-Secure Nested Paging

eine Funktion auf AMD EPYC™ Prozessoren, auf den Instance-Typen M6a, C6a und R6a.

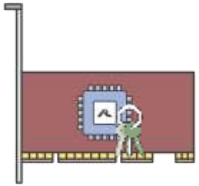
Sie stellt folgende Eigenschaften bereit:

Beglaubigung – AMD SEV-SNP ermöglicht es Ihnen, einen signierten Beglaubigungsbericht abzurufen, der ein kryptografisches Maß enthält, das verwendet werden kann, um den Status und die Identität der Instanz zu validieren, und dass sie auf echter AMD-Hardware ausgeführt wird.
https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf

Speicherverschlüsselung – Beginnend mit Prozessoren von AMD EPYC (Mailand), AWS Graviton2 und Intel Xeon Scalable (Ice Lake) wird der Instance-Speicher immer verschlüsselt. Instances, die für AMD SEV-SNP aktiviert sind, verwenden einen instanzspezifischen Schlüssel für ihre Speicherverschlüsselung

https://aws.amazon.com/de/about-aws/whats-new/2023/04/amazon-ec2-amd-sev-snp/

Relevanz von NITRO



AWS Nitro System API & Security Claims

Amazon Web Services, Inc.
Version 1.0 – April 11, 2023

1. There is no mechanism for a cloud service provider employee to log in to the underlying host.
2. No administrative API can access customer content on the underlying host.
3. There is no mechanism for a cloud service provider employee to access customer content stored on instance storage and encrypted EBS volumes.
4. There is no mechanism for a cloud service provider employee to access encrypted data transmitted over the network.
5. Access to administrative APIs always requires authentication and authorization.
6. Access to administrative APIs is always logged.
7. Hosts can only run tested and signed software that is deployed by an authenticated and authorized deployment service. No cloud service provider employee can deploy code directly onto hosts

As a matter of design, NCC Group found no gaps in the Nitro System that would compromise these security claims. All designs involve trade-offs, and AWS has chosen a design where the impact of a malicious compromise would be similar to a small-scale hardware failure.

AWS Service Terms
Last Updated: May 3, 2023

96. AWS Nitro System
AWS personnel do not have access to Your Content on AWS Nitro System EC2 instances. There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access Your Content on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance. Access to AWS Nitro System EC2 instance APIs – which enable AWS personnel to operate the system without access to Your Content - is always logged, and always requires authentication and authorization.

https://research.nccgroup.com/2023/05/03/public-report-aws-nitro-system-api-security-claims/

https://aws.amazon.com/service-terms/?nc1=h_ls

Einschränkung auf eine Nitro Instanzen möglich

Mit Service- Kontrollrichtlinien (SCPs) kann die Nutzung auf Nitro Instanzen beschränkt werden

(weitere Konfigurationen notwendig!)

```
"Effect": "Deny",
"Action": [
   "ec2:RunInstances"
],
"Resource": [
   "arn:aws:ec2:*:*:instance/*"
],
"Condition": {
   "StringNotLike": {
      "ec2:InstanceType": [
         "t2.*",
         "t3.*"
      ]
   }
}
```

DATENSCHUTZNACHWEISE ZERTIFIZIERUNGEN

CISPE CoC

European Regulators Green Light Pioneering GDPR Compliance Code for Cloud Infrastructure

by CISPE | May 19, 2021 | Latest News | 0 comments

Brussels, 20th May 2021 – Today, the European Data Protection Board (EDPB) comprised of all the European Data Protection Authorities (DPA) provided a favourable opinion that the CISPE Data Protection Code of Conduct complies with the General Data Protection Regulation(GDPR). Submitted by French DPA, CNIL, the CISPE Code is the first pan-European sector-specific code for cloud infrastructure service providers to reach this stage.

https://cispe.cloud/european-regulators-green-light-pioneering-gdpr-compliance-code-for-cloud-infrastructure/

https://aws.amazon.com/blogs/security/aws-announces-cispe-membership-and-compliance-with-first-ever-code-of-conduct-for-data-protection-in-the-cloud/

CISPE CoC

The GDPR requires in its Article 46 that data exporters shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR diversifies the appropriate safeguards that may be used by data exporters under Article 46 for framing transfers to third countries by introducing, amongst others, certification as a new transfer mechanism (Articles 42 (2) and 46 (2) (f) GDPR).

These guidelines provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification.

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en /

privacy shield – JA – NEIN - aber

3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass personenbezogene Daten in Drittländer ohne einen Angemessenheitsbeschluss nur dann übermittelt werden dürfen, wenn hierfür geeignete Garantien vorgesehen sind. Diese Garantien können beispielsweise in genehmigten Verhaltensregeln oder Zertifizierungsmechanismen als Transferinstrumente für Drittstaatentransfers bestehen.

Hierzu hat der Europäische Datenschutzausschuss (EDSA auf Basis der Vorarbeiten der Expert Subgroup International Transfers (ITS ESG) zwei entsprechende Leitlinien angenommen.

Zum einen handelt es sich um die Leitlinien für Zertifizierungen (Guidelines 07/2022 on certification as tool for transfers)und zum anderen um die für genehmigte Verhaltensregeln (Guidelines 04/2021 on codes of conduct as tools for transfers).

Damit hat der EDSA jetzt zu allen Transferinstrumenten („**geeignete Garantien**“ im Sinne des Art. 46 DSGVO) veröffentlicht.

Guidelines 07/2022 on certification as tool for transfers , abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.pdf

CISPE CoC

update

Der CISPE-Kodex wurde vom Europäischen Datenschutzausschuss (EDSA) geprüft und von der französischen Datenschutzbehörde (CNIL) genehmigt. Er bietet Unternehmen die Sicherheit, dass ihr Cloud-Infrastruktur-Dienstanbieter die Anforderungen erfüllt, die für in ihrem Auftrag verarbeitete personenbezogene Daten (Kundendaten) gemäß der DSGVO gelten. Der CISPE-Kodex erhöht auch die Messlatte für Datenschutz für Cloud-Dienste in Europa, indem er über die aktuellen DSGVO-Anforderungen hinausgeht. Zum Beispiel:

- **Daten in Europa: Der CISPE-Kodex geht über die DSGVO-Konformität hinaus, indem er Cloud-Infrastruktur-Dienstanbieter dazu verpflichtet, ihren Kunden die Wahl zu geben, Dienste zur Speicherung und Verarbeitung von Kundendaten ausschließlich im Europäischen Wirtschaftsraum (EWR) zu nutzen.**
- **Datenschutz: Der CISPE-Kodex verbietet Cloud-Infrastruktur-Dienstanbietern, Kundendaten für Data Mining, Profiling oder Direktmarketing zu verwenden.**
- Schwerpunkt auf Cloud-Infrastruktur: Der CISPE-Code adressiert die spezifischen Rollen und Verantwortlichkeiten von Cloud-Infrastruktur-Dienstanbietern (dies ist in allgemeineren Kodizes nicht abgebildet).

Für diese initial 52 nun 100 AWS-Dienste wurde nun unabhängig verifiziert, dass sie mit dem CISPE-Kodex konform sind. Der Überprüfungsprozess wurde von Ernst & Young CertifyPoint (EY CertifyPoint) durchgeführt, einer unabhängigen, weltweit anerkannten Überprüfungsstelle, die von der CNIL akkreditiert ist. AWS ist an die Anforderungen des CISPE-Kodex für die 52 deklarierten Dienste gebunden, und wir sind bestrebt, zusätzliche Dienste in den Umfang des CISPE-Compliance-Programms aufzunehmen.

https://aws.amazon.com/de/blogs/security/aws-cloud-services-adhere-to-cispe-data-protection-code-of-conduct/

Prüfung bzgl. Datenschutz = Datenschutznachweis

IDC CUSTOMER SPOTLIGHT

Beschleunigung in großem Maßstab - Die DB Group migriert auf eine rechtskonforme Cloud-Architektur von AWS

„Als nächstes wurde geprüft, ob AWS alle Vorschriften erfüllt, die die DB Group als zum Teil in staatlichem Besitz befindliches Unternehmen betreffen. Insbesondere ging es darum, ob der IaaS-Provider die deutschen Datenschutzregeln nach dem Bundesdatenschutzgesetz einhält. Die Prüfung durch DB Systel ergab, dass AWS dieses Kriterium erfüllte (und zwar zu diesem Zeitpunkt als einziger Provider vollständig).“

https://d1.awsstatic.com/analyst-reports/AWS%20DB%20Case%20Study%20German-Language.pdf https://www.heise.de/news/Warum-die-Bahn-jetzt-ihre-Daten-bei-Microsoft-und-Amazon-speichert-4940919.html

Berliner Verkehrsbetriebe (BVG) auf AWS

„Unsere von AWS entwickelte Lösung ermöglicht eine „tiefe Integration“ von Mobilitätsangeboten in einer App, sodass Passagiere in einer App nicht nur suchen, sondern auch buchen und bezahlen können.

Mit Jelbi müssen sich Fahrgäste nur einmal registrieren, um jeden Mobilitätsmodus in Berlin nutzen zu können – kein Hin- und Herwechseln zwischen Apps mehr.“

Michel Jakob Heider
Geschäftsführer von Jelbi

https://aws.amazon.com/de/solutions/case-studies/berliner-verkehrsbetriebe-aws-is-how/

https://www.jelbi.de/datenschutz/

Dokumentation bzgl. Datenschutz

EU-DSGVO bei Personio

Whitepaper

zum Download

IT-Infrastruktur und Einsatz von AWS bei Personio

Whitepaper

zum Download

Inhaltsverzeichnis

Personio setzt Amazon Web Services Europe (AWS) als **Hosting-Provider** ein.

Die Rechenzentren von AWS sind unter anderem **DIN ISO/IEC 27001** und **DIN ISO/IEC 27018** zertifiziert und gewährleisten höchste datenschutzrechtliche Sicherheit.

AWS erfüllt nicht nur strenge **Sicherheits- und Compliance-Anforderungen**, sondern ermöglicht die Steigerung der **Stabilität** und Skalierbarkeit unserer Infrastruktur.

Alle Kundendaten werden auf **Servern innerhalb der europäischen Union** gespeichert.

Um die Sicherheit zu gewährleisten, werden alle Daten im Ruhezustand **(Encryption at rest)** und bei der Übertragung über öffentliche Netzwerke verschlüsselt **(Encryption in Transit)**.

Personio ergreift **zusätzliche technische und organisatorische Maßnahmen**, um die Sicherheit der Verarbeitung zu gewährleisten.

https://assets.ctfassets.net/p03bi75xct27/56BL9DoIRmvpSdMGaoXOGb/d37538c416fad1dd671eacba1b7073e6/2022_AWS_DataSecurity_Brochure_DE-2.pdf

https://www.personio.de/datenschutz/ https://www.personio.de/datenschutz/#whitepaper-datenschutz

Healthcare-Daten in der AWS-Cloud?

Healthcare-Daten in der AWS-Cloud? Mission possible – hier ist wie

26. Apr. 2022

By Prof. Dr. Dr. Christian Dierks

Sie sind in Healthcare unterwegs und erwägen den Einsatz von AWS Services?

Getriggert von der Diskussion über die Zulässigkeit der Verarbeitung personenbezogener Gesundheitsdaten in Cloudlösungen haben wir uns die Rahmenbedingungen bei AWS angesehen und die entscheidenden Fragen im Hinblick auf einen datenschutzkonformen Einsatz gestellt und beantwortet. Hier ein Vorspann:

- Ist es in Deutschland erlaubt, Gesundheits- und Sozialdaten in der Cloud zu speichern?
- Erfüllt das DPA von AWS die Anforderungen des Art. 28 DSGVO?
- Kann ich bei der Nutzung von AWS die Anforderungen des § 80 SGB X erfüllen?

Neugierig geworden? Erfahren Sie mehr mit der ausführlichen Analyse in den beiden Q+A-Dokumenten, die frei zum Download bereitstehen.

Cloud geht nicht – gibt's nicht.

26. Apr. 2022

Healthcare-Daten in der AWS-Cloud?
Mission possible – hier ist wie

DIERKS + COMPANY

Q&A für AWS-Kunden - Krankenhäuser

Im Auftrag von	Amazon Web Services EMEA SARL
Projektname	03096 AWS01 Q&A
Thema	Q&A zur Speicherung und Verarbeitung von Gesundheitsdaten in der AWS-Cloud durch Krankenhäuser

DIERKS + COMPANY

Q&A für AWS-Kunden - HealthCare

Im Auftrag von	Amazon Web Services EMEA SARL
Projektname	03096 AWS01 Q&A
Thema	Q&A zur Speicherung und Verarbeitung von Sozial- und Gesundheitsdaten in der AWS-Cloud durch Kunden im Healthcare-Bereich
Autor	Dierks+Company Rechtsanwaltsgesellschaft mbH
Datum	25. März 2022

https://www.dierks.company/de/spotlights/healthcare-daten-in-der-aws-cloud-mission-possible-hier-ist-wie/

https://www.dierks.company/de/beyond/dc-spotlights

Dokumentation bzgl. Datenschutz

Datenschutz der Recare Plattform

Der Schutz Ihrer Daten steht bei uns an erster Stelle.

Simpliant

Recare wird von der externen Datenschutz- und IT-Sicherheitsberatung Simpliant GmbH unterstützt.

Recare erfüllt im vollen Umfang die DSGVO

https://recaresolutions.com/datenschutz-recare-plattform/ https://recaresolutions.com/datenschutz/ https://www.youtube.com/watch?v=dBJgZoG9KT8

Cloud-Referenzprojekt

Projektziel

Das Krankenhaus und zwei verbundene MVZ erhält nach Verkauf aus einem Konzern an einen privaten Träger eine eigenständige, wirtschaftlich darstellbare, hochsichere IT-Infrastruktur. Die Anwendungslandschaft inklusive Krankenhausinformationssystem (KIS) ist neu gestaltet und an die Bedürfnisse der Einrichtungen angepasst

Vorgehen

Nach Evaluierung des Anforderungskatalogs erfolgte die Planung und Umsetzung eine auf AWS-Services basierenden Virtuellen Private Cloud (VPC), durchgängig verschlüsselt mit Customer managed Keys (at-rest und in-transit). Eine Altdaten-Migration wird nur für Bilddaten und digitale Patientendokumente als wirtschaftlich erachtet. Eine Migration der Patientenstammdaten von KIS zu KIS erfolgt nicht.

Aktueller Stand

Die Kernapplikationen Krankenhausinformationssystem und Rö-Bild-Archiv sind erstellt und soweit möglich, Altdaten migriert. Die Go-live-Termine sind festgelegt.

Der Altdaten-Abgleich für Wiederkehrer (zur Gewährleistung des Zugriffs auf Altdokumente) erfolgt über FHIR-Ressourcen in einem Healthlake in der VPC.

Ausblick und Vision

Die Datenhaltung erfolgt zentral über den Healthlake, nicht über verteilte Datenbanken. Die Notwendigkeit von Kommunikation zwischen Haupt- und Subsystemen unter Zuhilfenahme von Schnittstellenvermittlern entfällt.

Das OBERENDER Cloud-Paket

KITE CONSULT

Fachklinikum Mainschleife

Orthopädie und Chirurgie

KITE CONSULT OBERENDER

aws

Cloud-Referenzprojekt

Krankenhaus-IT EXTRA JOURNAL — Der Newsletter für die IT im Gesundheitswesen

Erstes Klinikum in Deutschland betreibt KIS in der Cloud

Veröffentlicht 28.03.2023 12:00, Kim Wehrs

Das Fachklinikum Mainschleife betreibt sein neues Krankenhaus-Informationssystem (KIS) CLINIXX® seit Jahresbeginn in der AWS (Amazon Webservices) Cloud. Damit ist die Fachklinik für Orthopädie, Unfallchirurgie und minimalinvasive Allgemeinchirurgie deutschlandweit das erste Krankenhaus, das sein KIS in der Cloud betreibt. Weil das Krankenhaus aufgrund eines Trägerwechsels die Chance hatte, die komplette IT-Infrastruktur neu aufzustellen, wurden alle Software-Lösungen mit dem Fokus auf Web- und Cloudfähigkeit sowie auf vollständige Informationssicherheit geprüft. Neben dem CLINIXX® KIS der AMC Holding GmbH erhielten zwei weitere Mitglieder der United Web Solutions e. V. den Zuschlag für die Digitalisierung der ärztlichen und pflegerischen Prozesse. In den kommenden Monaten folgt die Einführung der ebenfalls webfähigen Speziallösungen für Pflegeplanung und -dokumentation apenio® der gleichnamigen apenio GmbH & Co. KG sowie die digitale Medikation mit ID MEDICS® von ID Berlin.

Umstieg von IS-H und i.s.h.med auf ein webbasiertes KIS in 7 Monaten

Das OBERENDER Cloud-Paket — KITE CONSULT

Fachklinikum Mainschleife
Orthopädie und Chirurgie

„Vor der Entscheidung für die AWS Cloud, haben wir diese auf die Einhaltung der strengen bayerischen Datenschutzrichtlinien hin geprüft. Dafür wurden gemeinsam mit der Firma Kite Consult, einem zertifizierten AWS Select Consulting Partner, mehrere Audits erfolgreich durchgeführt.“ erläutert Grube

KITE CONSULT OBERENDER

https://www.krankenhaus-it.de/item.2382/erstes-klinikum-in-deutschland-betreibt-kis-in-der-cloud.html
https://e-health-com.de/details-news/erstes-klinikum-in-deutschland-betreibt-kis-in-der-cloud/

aws

Klinische Studien brauchen gute Daten

Climedo Health erfasst Patienten-zentrierte, konforme und sichere klinische Daten mit AWS

2022

Der deutsche Anbieter von Software für elektronische Datenerfassung (Electronic Data Capture, EDC) Climedo Health nutzte AWS, um sichere, cloudnative und skalierbare Lösungen zur besseren Erfassung und Verwaltung klinischer Daten zu erstellen, die von Pharmaunternehmen, Medizinprodukteherstellern, Krankenhäusern und rund 150 Gesundheitsämtern verwendet werden. Das schnell wachsende Unternehmen beschleunigte die klinischen Studien seiner Kunden und nahm in kurzer Zeit Hunderttausende von Patienten auf.

Wir haben uns für AWS entschieden, weil es uns hilft, die Datenschutzstandards zu erfüllen und die Skalierbarkeit bietet, die wir brauchen."

Benjamin Sauer
Head of Backend Engineering bei Climedo Health

https://aws.amazon.com/de/solutions/case-studies/climedo-case-study/

Klinische Studien brauchen gute Daten

Climedo

Das digitale Symptom-Tagebuch wurde von der Climedo Health GmbH in Abstimmung mit dem Bundesministerium für Gesundheit (BMG), sowie unter Einbezug des Robert-Koch-Institut (RKI), des Bundesamtes für Sicherheit in der Informationstechnik (BSI), dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und der Akademie für öffentliches Gesundheitswesen – entwickelt.

Bundesministerium für Gesundheit

Alle personenbezogenen Daten der betroffenen Kontaktpersonen werden für jedes einzelne Gesundheitsamt separat auf den Hochsicherheitsservern des Informationstechnikzentrum Bund (ITZ-Bund) gespeichert. Die nicht -personenbezogenen Daten werden auf den Servern der AWS in Deutschland
gespeichert.

Die Email des Patienten wird in AWS verschlüsselt gespeichert.

https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/O/OEGD/Climedo_Projektsteckbrief.pdf

aws

Schüler-Daten in der AWS-Cloud!

Information to our customers about GDPR

The EU's General Data Protection Regulation (GDPR), approved by the European Parliament in 2016, is the most important change within data protection regulation in 20 years. It replaces the Data Protection Directive 95/46/EC and local law and regulations across the EU/EEA. The new regulation is designed to strengthen the individual's rights to privacy and harmonize data privacy laws across Europe.

itslearning has been committed to data privacy since it was founded in 1999 and welcomes the new regulation. We will keep doing our part to ensure that all our customers are GDPR compliant. There is a big, untapped potential in using technology and cloud services to improve teaching practices and learning outcomes. One of the keys to unlocking this potential is to earn the trust of teachers, students, and parents. In this sense, the increased focus on data protection and privacy due to GDPR is beneficial for all parties.

itslearning GDPR Commitment

We fully comply with the requirements for all of our services, including itslearning, Fronter and SkoleIntra to be GDPR ready. We have been working with GDPR for a long time to analyse the new regulation, and making the necessary changes to our services, procedures, and organization. During the previous months, we made available all documentation, contract addendums, and procedures needed to prove your GDPR compliance.
It is important to say that for the cloud services we provide to our customers and their end users, itslearning is what both existing and new EU regulation defines as a processor. As a processor we do not decide the purpose or lawfulness of the processing, we merely process data on our customers' behalf. The GDPR regulations force stricter requirements upon all processors of data.
Our commitment to GDPR requires that we work to:

- Ensure organisational and technical security for all services.
- Help you with the documentation needed to demonstrate compliance and inform your users.
- Provide you with new contract addendums that comply with GDPRs requirements for Data Processing Agreements (DPA)
- Provide the necessary support for you when your users are executing their data subject rights. You can find more information on the GDPR Data Request page on our Support site.

itslearning has a Data Protection Officer (DPO) as defined under GDPR. In addition to monitoring our own compliance and providing advice and training to our own staff, our DPO is available to our customers and their DPOs to discuss data privacy issues.
Contact details for our DPO:
Riikka Turunen

https://itslearning.com/global/your-data-matters/gdpr/

Schüler-Daten in der AWS-Cloud!

Schleswig-Holstein extends contract with itslearning

The extension of the contract ensures the further development of a more flexible teaching and learning environment across the state.

Bergen, May 28, 2021 – The Nordic learning platform provider itslearning has won a three-year contract to deliver the learning management system for schools in the German state of Schleswig-Holstein. itslearning will be available for 400,000 students and teachers with a wide range of educational tools and remote learning solutions.

https://itslearning.com/global/news/schleswig-holstein-extends-contract-with-itslearning/

Welcome to the itslearning family Baden-Württemberg!

PRESS RELEASE

Strategic move to provide all schools in the state with an alternative pedagogical and scalable digital learning environment

Bergen, Dec 9, 2020 – itslearning has been selected by Germany's third largest state Baden-Württemberg as its new statewide learning management system to support teachers and students with a wider range of educational and teaching options.

Work has begun in close cooperation with the State Ministry of Education to begin rolling out the LMS for 50,000 users in the first phase, with a potential final count of 1.6 million.

https://itslearning.com/global/news/baden-wurttemberg-selects-itslearning/

Schnelle Auszahlung von Fördermitteln ermöglichen

Die öffentliche Hand hat auf Bundes- und Landesebene mit umfassenden Hilfsprogrammen auf diese Auswirkungen reagiert.

- Pandemie erzeugt massive Rezession in Deutschland
- Schnelle operative Umsetzung von Förderprogrammen
- Digitale Lösung für Antrag und Auszahlung
- Kurzfristige Bereitstellung einer skalierbaren, zuverlässigen Cloud-Plattform

Überall in der Welt leiden Volkswirtschaften unter den Auswirkungen der Corona-Pandemie. Für Deutschland errechnete das ifo-Institut Ende März 2020 Kosten, die sich auf über 700 Mrd. Euro summieren können. Durch Produktionsausfälle und Kurzarbeit wird das Bruttoinlandsprodukt bei einem 2-monatigen Shutdown zwischen 7,2 und 14 Prozentpunkten einbrechen. Durch den Wirtschaftseinbruch sind eine Million Arbeitsplätze in Gefahr.

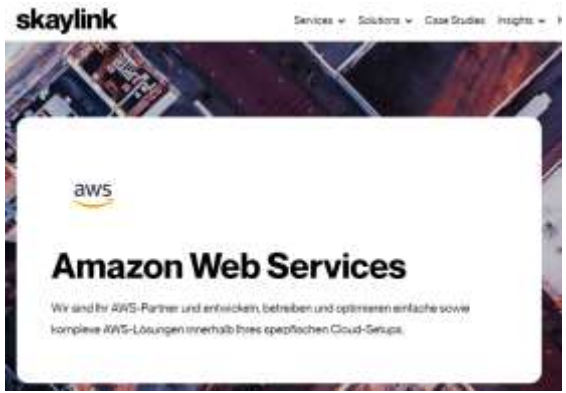
https://www.t-systems.com/de/de/referenzen/cloud-und-infrastructure/rechenzentrum-aws

Partner bzgl. Sicherheit & Datenschutz

https://www.t-systems.com/resource/blob/491654/8af70086b8fc61813ae675da75384e92/WP-white-paper-T-Systems-White-Paper-AWS-Security-Compliance-de-data.pdf

https://aliceandbob.company/work/case-studies-e-commerce-encrypt-everything/
https://aliceandbob.company/wp-content/uploads/2021/09/Checklist-GDPR-Compliance-V6.pdf

https://www.tecracer.com/

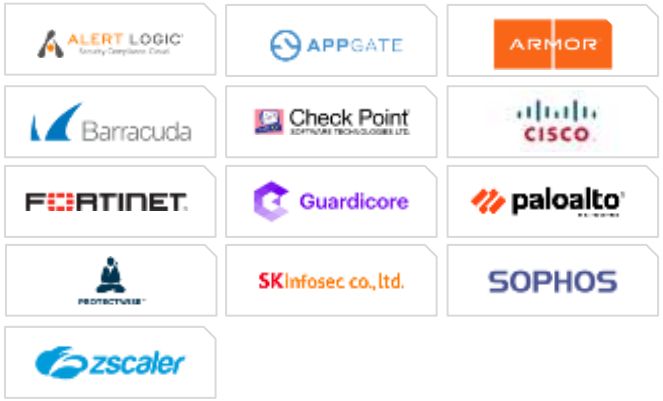


https://www.skaylink.com/solutions/technologie-partner/aws/

https://nordcloud.com/solutions/reduce-risk-cost/improve-security-compliance/

Largest ecosystem of security partners and solutions

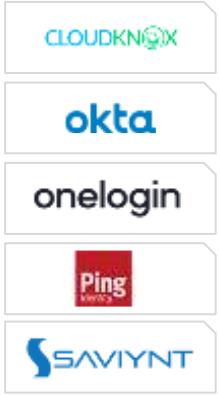
Network & infrastructure security



Host & endpoint security

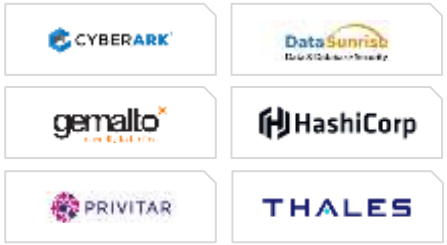
Application security

Identity & access control



Vulnerability & configuration analysis

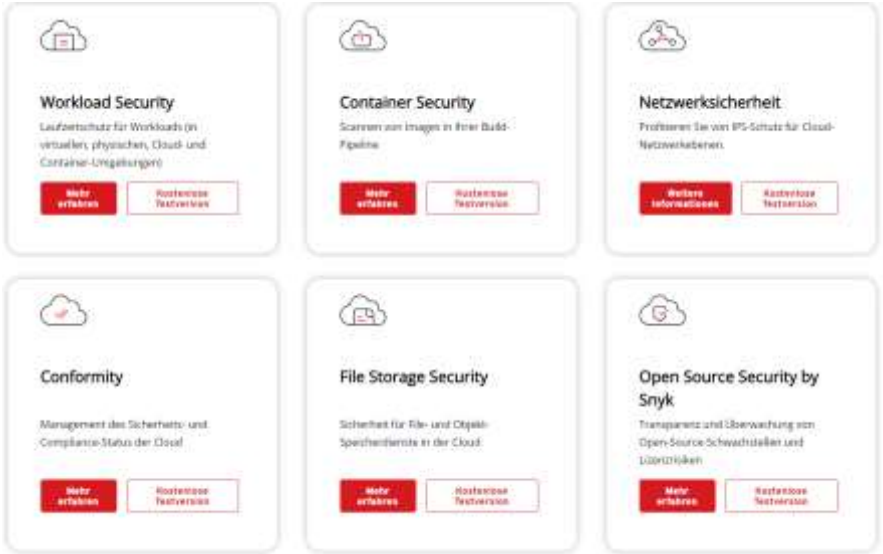
Data protection & encryption

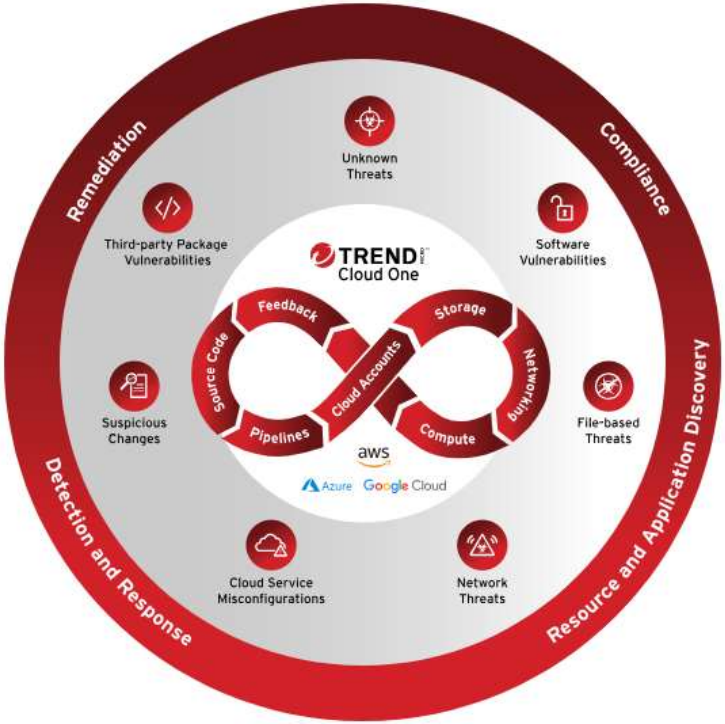


Logging, monitoring, SIEM, threat detection, & analytics

aws

Largest ecosystem of security partners and solutions





https://www.trendmicro.com/de_de/business/products/hybrid-cloud.html

CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT

CLOUD ACT

Erläuterung zum CLOUD Act

The CLOUD Act Does Not Take Precedence Over Existing Laws

The CLOUD Act does not ignore, supersede, or change another country's local laws. In fact, the CLOUD Act recognizes the right for service providers to challenge requests that conflict with another country's laws or national interests.

26. Will U.S. law enforcement go directly to service providers to obtain information of an employee of an enterprise when the enterprise is not otherwise suspected of committing a crime?

The CLOUD Act does not change U.S. law or practice with regard to enterprise customer data. The U.S. Department of Justice's Computer Crime and Intellectual Property Section has publicly advised that "prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought." For more information about the factors that influence the Department's approach to seeking enterprise data, see: https://www.justice.gov/criminal-ccips/file/1017511/download.

29. Does the CLOUD Act require providers to decrypt data in response to law enforcement requests?

No. The CLOUD Act is "encryption neutral." It does not create any new authority for law enforcement to compel service providers to decrypt communications. Neither does it prevent service providers from assisting in such decryption, or prevent countries from addressing decryption requirements in their own domestic laws.

19. What is necessary under the Stored Communications Act to obtain a warrant for stored content?

The Stored Communications Act permits law enforcement to obtain a warrant to require a provider to disclose the stored contents of a user account. Warrants must meet demanding and highly privacy-protective constitutional requirements. The warrant must be supported by a statement sworn under penalty of perjury showing probable cause that the place searched will contain particular things subject to seizure; must state with particularity the crime that is alleged, the information to be disclosed and the evidence to the seized; and must be approved by an independent judge. The CLOUD Act did not change these existing high standards under U.S. law. "Probable cause" is a particularly exacting standard, among the most demanding in the world.

20. Will a warrant issued under the Stored Communications Act allow the U.S. to scoop up large amounts of data indiscriminately?

No. The CLOUD Act did not alter or expand the historical scope of warrants issued under U.S. law. Indiscriminate or bulk data collection is not permitted.

The CLOUD Act clarified that U.S. law requires that providers subject to U.S. jurisdiction disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data. This ensured consistency with U.S. obligations under Article 18(1) of the Budapest Cybercrime Convention, aligning the United States with the more than 60 other parties to the Convention.

US department of justice: https://www.justice.gov/criminal-oia/page/file/1153466/download additional explanations

https://www.justice.gov/criminal-oia/page/file/1152896/download the CLOUD Act

“Vorteile” des CLOUD Act

FOR IMMEDIATE RELEASE — Thursday, September 26, 2019

Joint US-EU Statement on Electronic Evidence Sharing Negotiations

U.S. Department of Justice and European Commission officials met yesterday to begin formal negotiations on an E.U.-U.S. agreement to facilitate access to electronic evidence in criminal investigations. After a productive first discussion, there was agreement to regular negotiating rounds with the view to concluding an agreement as quickly as possible. Progress will be reviewed at the next E.U.-U.S. Justice and Home Affairs Ministerial in December.

European Commissioner for Justice, Věra Jourová said, "I welcome the start of formal negotiations. Criminals use fast, modern technologies to organize their crimes and cover up their evidence. We need to work together with our American partners to speed up the access of our enforcement authorities to this evidence. This will strengthen our security, while protecting the data privacy and procedural safeguards of our citizens. The launch of negotiations marks an important step towards achieving this."

U.S. Attorney General William Barr said, "We are pleased that the Council adopted a mandate to authorize the Commission to negotiate an agreement with the United States on facilitating access to certain e-evidence, and that we have obtained authorization to negotiate with the European Union. This type of agreement can enhance public safety and national security by providing an improved and more rapid ability to identify and respond to criminal threats on both sides of the Atlantic, in a manner that assures respect for the rule of law, privacy, and civil liberties. The U.S. is committed to working with the E.U. on this important issue."

Component(s): Office of the Attorney General

Press Release Number: 19-1034

https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations

Erklärung | 26. September 2019 | Brüssel

Strafjustiz: Gemeinsame Erklärung zum Start der Verhandlungen zwischen der EU und den USA über die Erleichterung des Zugangs zu elektronischen Beweismitteln

Seiteninhalte

- Seitenanfang
- PDF-Druckversion
- Kontaktpersonen für die Medien

Beamte der Europäischen Kommission und des US-Justizministeriums kamen gestern zusammen, um förmliche Verhandlungen über ein Abkommen zwischen der EU und den USA aufzunehmen, das den Zugang zu elektronischen Beweismitteln bei strafrechtlichen Ermittlungen erleichtern soll. Nach einer konstruktiven ersten Aussprache bestand Einvernehmen über die Aufnahme regelmäßiger Verhandlungsrunden, um schnellstmöglich zu einem Abkommen zu gelangen. Die Justiz- und Innenminister der EU und der USA werden auf ihrer nächsten Tagung im Dezember den Fortgang der Verhandlungen erörtern.

https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_19_5890

The Ability to Quash is Very Limited

It should also be noted that the ability of a CSP to seek to quash a CLOUD Act warrant for access to a customer's or subscriber's information only applies if:

- The person/entity is not a U.S. citizen and does not reside in the U.S.
- The required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government

https://dipbt.bundestag.de/doc/btd/19/153/1915374.pdf
https://dip21.bundestag.de/dip21/btd/19/149/1914921.pdf

Foreign Sovereign Immunities Act = FSIA

The **Foreign Sovereign Immunities Act** (**FSIA**) of 1976 is a United States law, codified at Title 28, §§ 1330, 1332, 1391(f), 1441(d), and 1602–1611 of the United States Code, that establishes the **limitations** as to whether a **foreign sovereign nation** (or its political subdivisions, agencies, or **instrumentalities**) may be sued in U.S. courts—federal or state.

(In international law, government protection against lawsuits in foreign courts is known as state immunity; government immunity in domestic courts is known as sovereign immunity.)

It also establishes specific procedures for service of process, attachment of property and execution of judgment in proceedings against a foreign state. The FSIA provides **the exclusive basis and means to bring a lawsuit against a foreign sovereign** in the United States.

https://en.wikipedia.org/wiki/Foreign_Sovereign_Immunities_Act
https://web.archive.org/web/20150627110441/http://usun.state.gov/documents/organization/218088.pdf

Foreign Sovereign Immunities Act = FSIA

The CLOUD Act did not change cloud providers' ability to protect their customers

AWS is vigilant about its customers' privacy and security. We are committed to providing all customers, including governmental agencies who trust us with their most sensitive content, with the most extensive set of security services and features to help ensure complete control of their data. The CLOUD Act did not alter or weaken this commitment. On the contrary, the CLOUD Act recognizes the right of cloud providers to challenge requests that conflict with another country's laws or national interests and requires that governments respect local rules of law. **Additionally, foreign governments concerned about the risk of government data disclosure may be entitled to sovereign immunity. The United States recognizes that under the principle of sovereign immunity foreign governments have effective legal means under U.S. law to prevent disclosure of their data.**

https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/

Government Requests for Data

- Government agencies seeking access to data of another entity generally will address any request for information directly to that entity
- In certain instances law enforcement entities may direct requests to third party providers
- **AWS is vigilant about protecting our customer content**, regardless of where a request for content comes from or who the customer is
- **AWS will not disclose customer** content unless required to do so to comply with a legally valid and binding order, such as a subpoena or a court order
- **AWS carefully examines each request** to authenticate its accuracy and verify that it complies with applicable law
- **AWS will challenge requests that are overbroad**, exceed the requestor's authority, or do not fully comply with applicable law
- Unless prohibited by law, **AWS also attempts to redirect the request directly to the customer**, providing the customer with an opportunity to take action against the request

https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

Amazon Law Enforcement Guidelines

Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course.

Amazon distinguishes between content and non-content information.

- We produce non-content information only in response to valid and binding subpoenas.
- We do not produce content information in response to subpoenas.
- **We may produce non-content and content information in response to valid and binding search warrants.**

"Non-content" information means subscriber information such as name, address, email address, billing information, date of account creation, and certain purchase history and service usage information.

"Content" information means the content of data files stored in a customer's account.

https://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Amazon & AWS Information Request Report

Types of Requests:

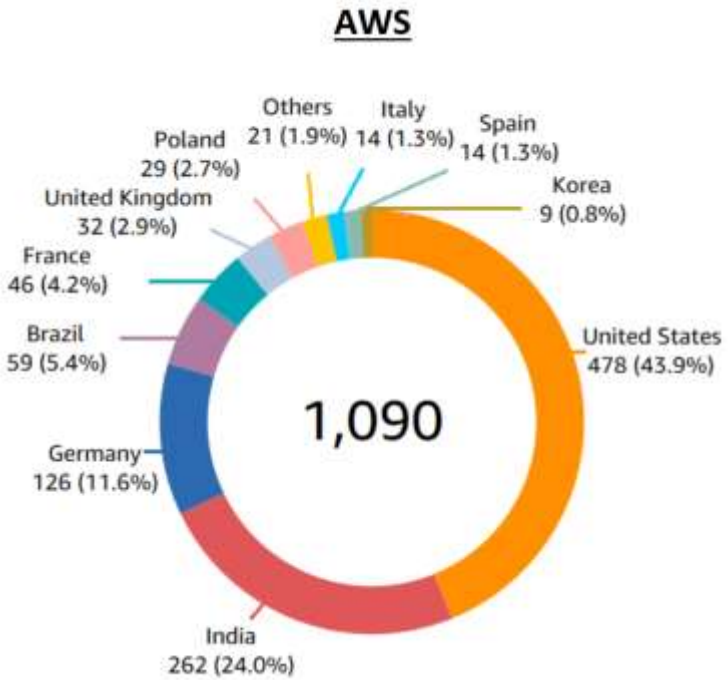
Subpoenas (including their equivalent in non-U.S. countries) are valid and binding legal demands for information or documents usually issued without substantive review by a judge or magistrate. Amazon does not produce content information in response to subpoenas.

Search warrants (including their equivalent in non-U.S. countries) are issued by courts upon a showing of probable cause or equivalent non-U.S. standards and must specifically identify the information to be produced. Amazon may produce non-content and content information in response to search warrants.

Court orders are valid and binding orders issued by courts other than search warrants. Amazon's response to court orders depends on the nature of the order, and Amazon may produce non-content and content information in response to court orders.

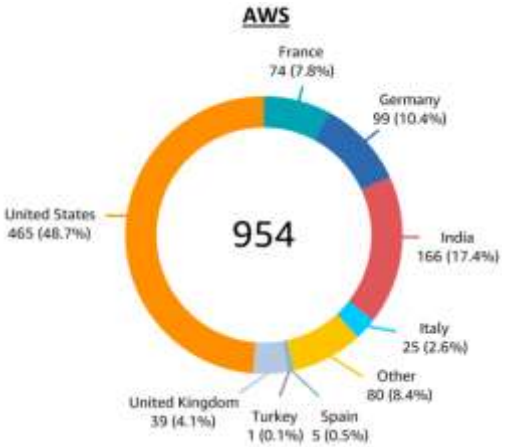
https://aws.amazon.com/de/compliance/amazon-information-requests/

Amazon & AWS Information Request Report



https://d1.awsstatic.com/Security/pdfs/Amazon_Information_Request_Report.pdf Published January 31, 2023

AWS Information Request Report



Q1 2022

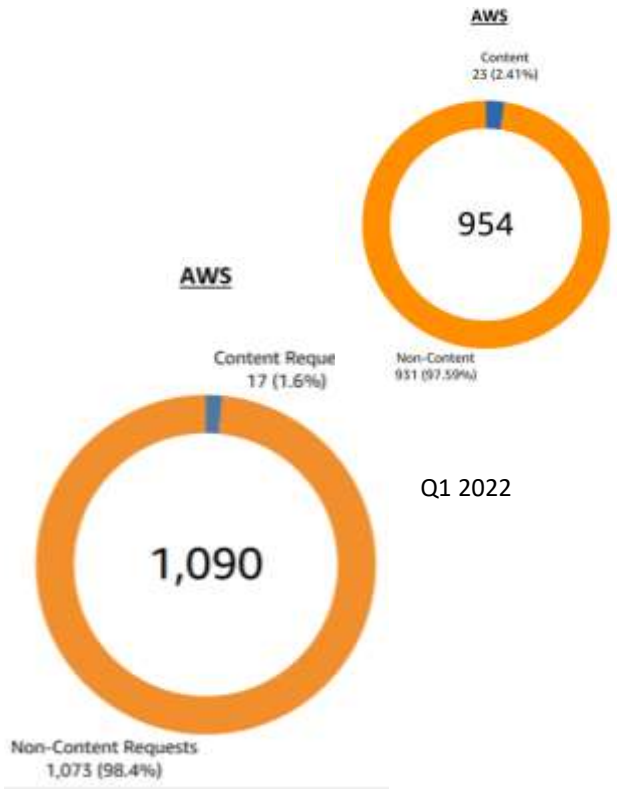
https://d1.awsstatic.com/Security/pdfs/Amazon_Information_Request_Report.pdf Published January 31, 2023

AWS Information Request Report

Non-content information mainly includes basic subscriber information (such as name, address, email address, billing information, and date of account creation), certain retail purchase history, and AWS service usage information. A non-content response might include basic subscriber information or no information.

Content information mainly includes the content of data files stored in a retail customer's account (such as a customer's photos) or, in the case of AWS, the content that a customer transfers for processing, storage, or hosting in connection with AWS services and any computational results.

Q2 2021

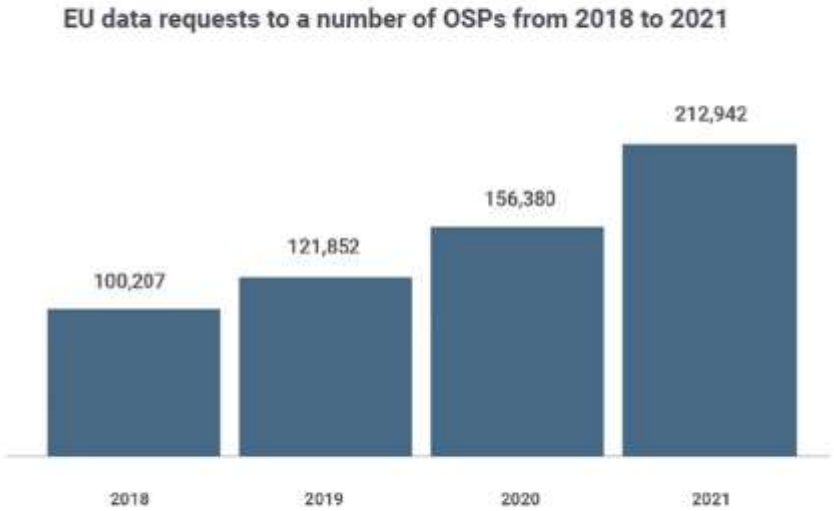


Q1 2022

https://d1.awsstatic.com/Security/pdfs/Amazon_Information_Request_Report.pdf Published January 31, 2023

EU initiated Information Request number

- 7 Online Service Providers analysed
- +36% increase
- 65% of requests submitted by Germany and France



Europol Unclassified – Basic Protection Level

UNCLASSIFIED

Amazon & AWS Information Request Report

Frequently Asked Questions

National Security Requests

National security requests include U.S. National Security Letters ("NSLs") and requests issued under the Foreign Intelligence Surveillance Act ("FISA"). Amazon's responses to these requests depend on the nature of the request. Amazon reports the numbers of such requests within certain ranges permitted by law. These requests are not included within the data presented above. The reporting range is 0-249 for all national security requests made to Amazon (including AWS).

Does the data above include requests received via the Mutual Legal Assistance Treaty ("MLAT") process?

Yes. Amazon includes MLAT requests as U.S. requests unless the country of origin is identified in the request.

Does the CLOUD Act change how Amazon responds to requests?

No. The CLOUD Act amended the Stored Communications Act to clarify that the U.S. government may seek to require U.S.-based service providers to disclose data that is in their "possession, custody, or control" regardless of whether the data is located within or outside of the United States. The CLOUD Act does not change any of the legal and privacy protections that apply to law enforcement requests for data. Amazon continues to object to overbroad or otherwise inappropriate requests as a matter of course regardless of where data is located.

How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States? **None**

https://d1.awsstatic.com/Security/pdfs/Amazon_Information_Request_Report.pdf Published January 31, 2023

Amazon & AWS Information Request Report

AWS Security Blog

AWS and EU data transfers: strengthened commitments to protect customer data

by Stephen Schmidt | on 17 FEB 2021 | in Announcements, Foundational (100), Security, Identity, & Compliance | Permalink | Comments | Share

Our **strengthened contractual commi**tments include:

- **Challenging law enforcement requests**: We will challenge law enforcement requests for customer data from governmental bodies, whether inside or outside the EEA, where the request conflicts with EU law, is overbroad, or where we otherwise have any appropriate grounds to do so.
- **Disclosing the minimum amount necessary**: We also commit that if, despite our challenges, we are ever compelled by a valid and binding legal request to disclose customer data, we will disclose only the *minimum amount* of customer data necessary to satisfy the request.

These commitments are automatically available to all customers using AWS to process their customer data, with no additional action required, through a new supplementary addendum to the AWS GDPR Data Processing Addendum.

https://aws.amazon.com/de/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

Amazon & AWS Information Request Report

Dealing with investigation requests from government agencies

Objective: *Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
INQ-01 Legal Assessment of Investigative Inquiries	AWSCA-13.23	Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.	-
INQ-02 Informing Cloud Customers about Investigation Requests	AWSCA-13.25	The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.	-
INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests	AWSCA-13.25	Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the proviso that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.	-
INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests	AWSCA-13.25	The Cloud Service Provider's procedures establishing access to or disclosing data of cloud customers in the context of investigation requests from governmental agencies ensure that the age or insight into the data that is the subject of th If no clear limitation of the data is possible, the Cloud Service Provider anonymises or pseudonymises the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.	-

Fragen?

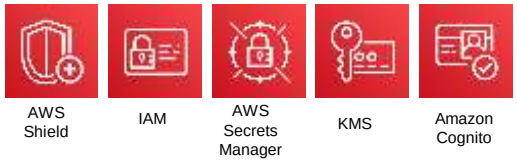
Vielen Dank
für Ihre
Aufmerksamkeit

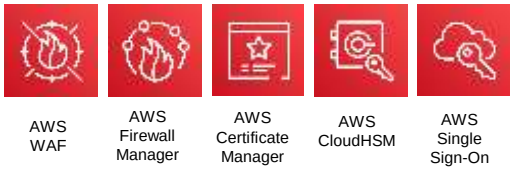
AWS Foundational and Layered Security Services (NIST)

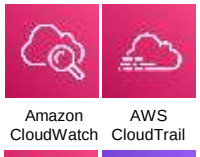
Identifizieren → Schützen → Erkennen → Response → Recover

Automatisieren

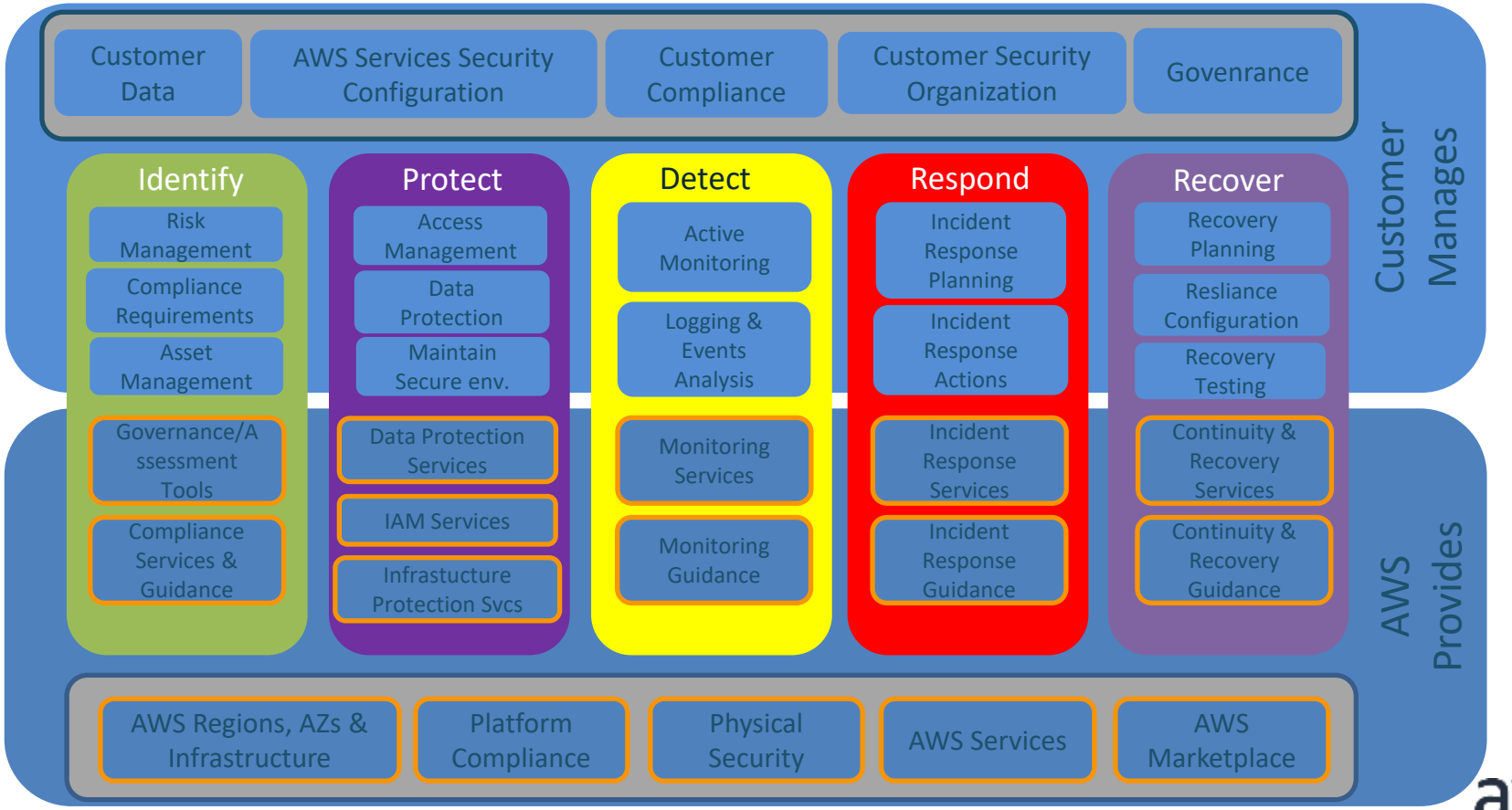
Untersuchen







AWS General Security Operating Model



Controls for Detect

Amazon GuardDuty	This control detects reconnaissance activity, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known, bad IP address.
Amazon Detective	Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.
Amazon CloudWatch, CloudWatch Logs, CloudTrail + Insights, Reporting & Third-Party Tools	These controls monitor, detect, visualize, and receive notifications of attacks, and respond to changes in your AWS resources
AWS Security Hub	This control gives you a comprehensive view of your high priority security alerts and compliance status across AWS accounts.
AWS Security Hub Partners	AWS Security Hub APN Partner products are a complement to Amazon GuardDuty.
AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config	When new AWS assets are created, or if malware is installed with a regular package, the AWS System Manager Inventory identifies it and sends it to AWS Config for evaluation.
Third-Party Security Tools for Containers	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Partner Network Offerings – Anti-Malware Protection	These controls help to detect and block malicious payloads.

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

Controls for Deny

AWS Identity and Access Management (IAM) + IAM Policies and Policies Boundaries	These controls can be configured to provide strong, least-privilege and need-to know security principles for both the users and services that can access your resources. IAM privileges are required to either grant or deny privileges for AWS administrators and engineers.
AWS Organizations + Service Control Policies (SCPs) + AWS Accounts	These controls can be utilized to provide strong, least-privilege and need-to know security principles for both users and services across a multi-account structure. SCPs can be used to deny (but not grant) privileges, overriding the potential privileges granted via IAM. You can control the privileges of all principals in child accounts and organizational units.
Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies	These controls manage access to objects and can prevent upload of objects into the Amazon S3 bucket by malicious actors. Note that there are other AWS services, besides S3, that also have resource policies, such as Amazon Simple Queue Service and Amazon Simple Notification Service.
Amazon Cognito	This control provides temporary, limited-privilege end-user credentials to allow access to appropriate AWS services.
Bottlerocket	This control provides a minimized OS environment capable of running and managing containers, which provides no extraneous listeners or services.
Amazon EC2 – Linux, Security-Enhanced Linux (SELinux) – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux, FreeBSD – Hardening and Minimization	These controls disable or remove unused services and packages.
Amazon EC2 – Windows – User Account Control (UAC)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)	This control implements least-privilege account profiles.
Amazon EC2 – Windows –Device Guard	This control specifies which binaries are authorized to run on your server.
AWS Partner Network Offerings – Anti-Malware Protection	

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

Controls for Disrupt

Amazon Simple Storage Service (Amazon S3) Bucket Policies, Object Policies	These controls manage access to objects and prevent upload of malicious objects into the Amazon S3 bucket.
AWS Systems Manager State Manager	This control helps you to define and maintain consistent OS configurations.
Amazon EC2 – Linux, SELinux – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Windows – User Account Control (UAC)	UACs make it more difficult for malware to install and run.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)	This control implements least-privilege account profiles.
Amazon EC2 – Windows – Device Guard	This control specifies which binaries are authorized to run on your server.
AWS Partner Network Offerings – File Integrity Monitoring	This control helps to maintain the integrity of operating system and application files.
AWS Partner Network Offerings – Anti-Malware Protection	These controls help to detect and block malicious payloads.

Controls for Degrade

AWS Systems Manager State Manager	This control helps you to define and maintain consistent OS configurations.
Immutable Infrastructure – Short-Lived Environments	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

Controls for Deceive

Honeypot and Honeynet Environments	These controls help to degrade, detect, and contain attacks.
Honeywords and Honeykeys	When an attacker attempts to use stolen, false credentials, these controls help to detect and contain the attack, so you can recover faster.

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

Controls for Contain

AWS Organizations + Service Control Policies (SCPs) + AWS Accounts	These controls strong privilege boundaries (AWS accounts) and, the ability to override privileges at the Organization or organizational unit (OU) level. They allow users to implement least-privilege and need-to know security principles for both users and services across a multi-account structure. You can control all privileges in OUs and child accounts.
Amazon EC2 – Linux, SELinux – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – FreeBSD Trusted BSD – Mandatory Access Control	This control is a system policy that cannot be overridden, which mediates access to files, devices, sockets, other processes, and API calls.
Amazon EC2 – Linux – Role-Based Access Control (RBAC) and Discretionary Access Control (DAC)	This control implements least-privilege account profiles.
Linux cgroups, namespaces, SELinux	These controls enforce capability profiles, which prevent running processes from accessing files, network sockets, and other processes.
Third-Party Security Tools for Containers	This control implements advanced security protection and behavioral security solutions for containers.
Third-Party Security Tools for AWS Lambda Functions	This control implements advanced security protection and behavioral security solutions for Lambda functions.
AWS Container and Abstract Services	These controls can help you prevent access to underlying infrastructure by your customers and threat actors, and segregate your service instances.
Hypervisor-Level Guest-to Guest and Guest-to-Host Segregation	This control leverages the string isolation capabilities of the AWS hypervisor.

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

Controls for Respond

AWS Systems Manager State Manager	This control helps you to define and maintain consistent OS configurations.
AWS Systems Manager State Manager, or Third-Party or OSS File Integrity Monitoring Solutions on Amazon EC2	This control automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.
AWS Systems Manager State Manager, AWS Systems Manager Inventory, AWS Config	When new AWS assets are created, or if malware is installed with a regular package, the AWS System Manager Inventory identifies it and sends it to AWS Config for evaluation.
AWS Partner Network Offerings – File Integrity Monitoring	This control helps to maintain the integrity of operating system and application files.
AWS Lambda	A serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes.

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

Controls for Restore

WS Auto Scaling	This control adjusts capacity to maintain steady, predictable performance.
AWS Systems Manager State Manager	This control helps you to define and maintain consistent OS configurations.
AWS Partner Network Offerings – File Integrity Monitoring	This control helps to maintain the integrity of operating system and application files.
CloudFormation + Service Catalog	These controls help you to provision your infrastructure in an automated and secure manner. The CloudFormation template file serves as the single source of truth for your cloud environment.
Immutable Infrastructure – Short-Lived Environments	These controls rebuild or refresh your environments periodically to make it more difficult for an attack payload to persist.

https://docs.aws.amazon.com/whitepapers/latest/classic-intrusion-analysis-frameworks-for-aws-environments/classic-intrusion-analysis-frameworks-for-aws-environments.html

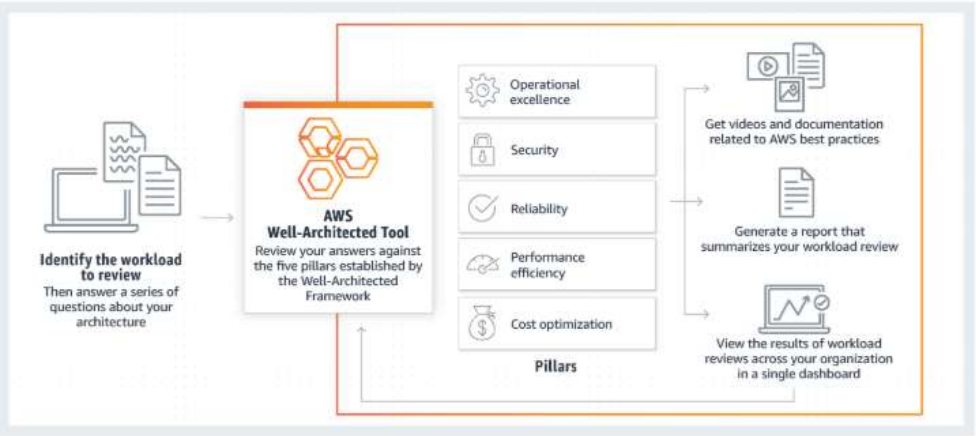
Consulting and technology competency partners

AWS Well-Architected Tool

Holen Sie sich architektonische Anleitung
Greifen Sie auf das Wissen und die Best Practices zu, die von AWS Solution Architects verwendet werden. Erhalten Sie Anleitungen zum Entwerfen und Betreiben von Workloads, die zuverlässig, sicher, effizient und kostengünstig sind.

Ermöglichen Sie eine konsistente Governance
Wenden Sie einen konsistenten Prozess an, um Ihre Cloud-Architekturen zu überprüfen und zu messen. Verstehen Sie potenzielle Risiken in Ihrer Arbeitslast und verwenden Sie die Ergebnisse der Überprüfung, um die nächsten Schritte zur Verbesserung zu ermitteln.

Architekturen kontinuierlich verbessern
Unterstützung der kontinuierlichen Verbesserung während des gesamten Workload-Lebenszyklus. Speichern Sie ganz einfach Meilensteine für Ihre Workload-Überprüfungen und verfolgen Sie Änderungen an Ihren Architekturen im Laufe der Zeit. Starten Sie bei Bedarf einen neuen Überprüfungsprozess, um sicherzustellen, dass Ihre Architektur mit den neuesten AWS-Best Practices übereinstimmt.

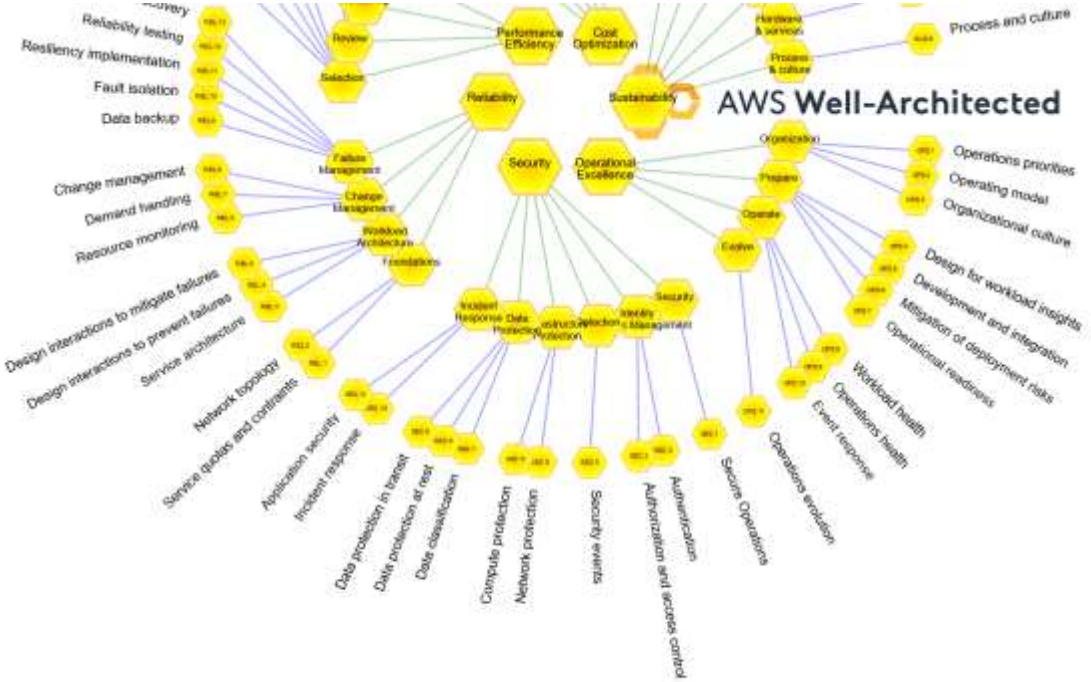


https://console.aws.amazon.com/wellarchitected/

AWS Well-Architected Tool

The Security pillar includes the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

The security pillar provides an overview of design principles, best practices, and questions. You can find prescriptive guidance on implementation in the Security Pillar whitepaper.



https://wa.aws.amazon.com/map.html

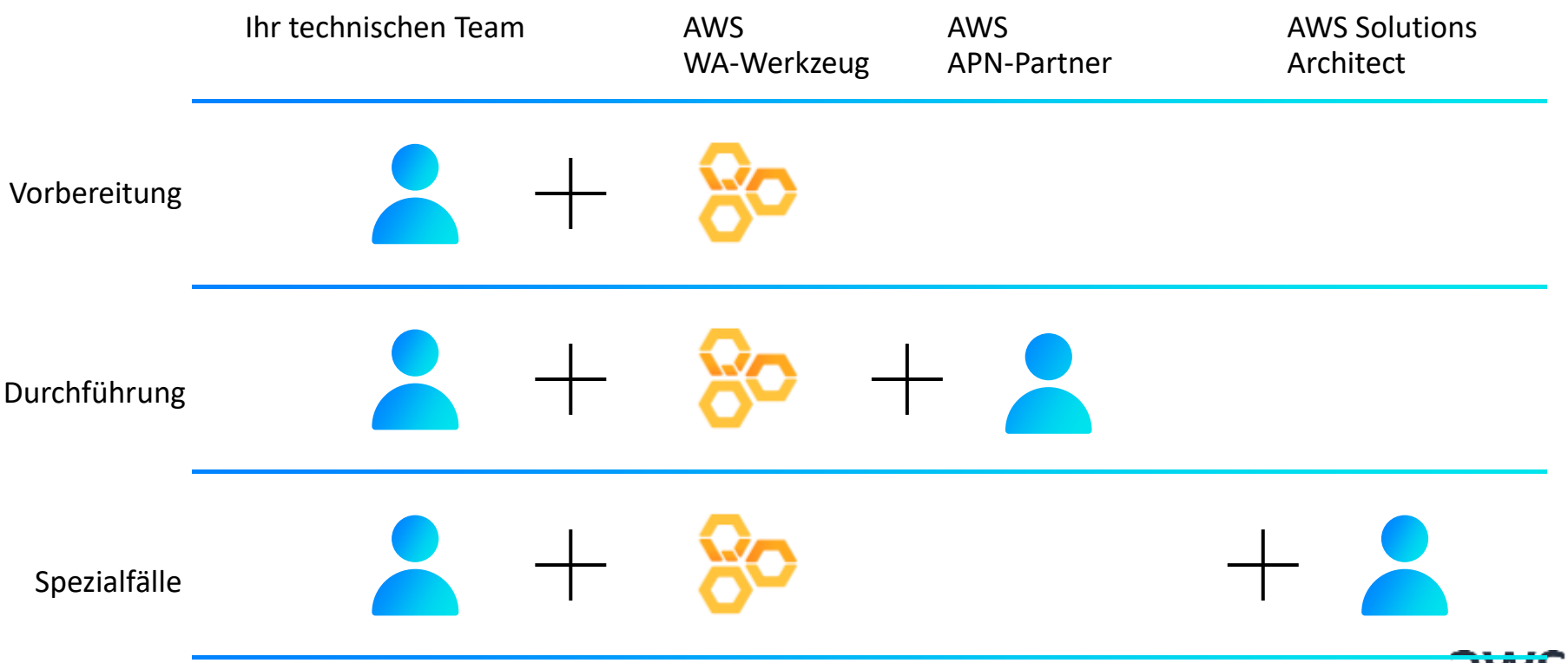
AWS Well-Architected Tool

Design Principles
There are seven design principles for security in the cloud:

•**Implement a strong identity foundation**: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize identity management, and aim to eliminate reliance on long-term static credentials.
•**Enable traceability**: Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
•**Apply security at all layers**: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code).
•**Automate security best practices**: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
•**Protect data in transit and at rest**: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
•**Keep people away from data**: Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data.
•**Prepare for security events**: Prepare for an incident by having incident management and investigation policy and processes that align to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

https://wa.aws.amazon.com/map.html

Phasen des Well-Architected Frameworks



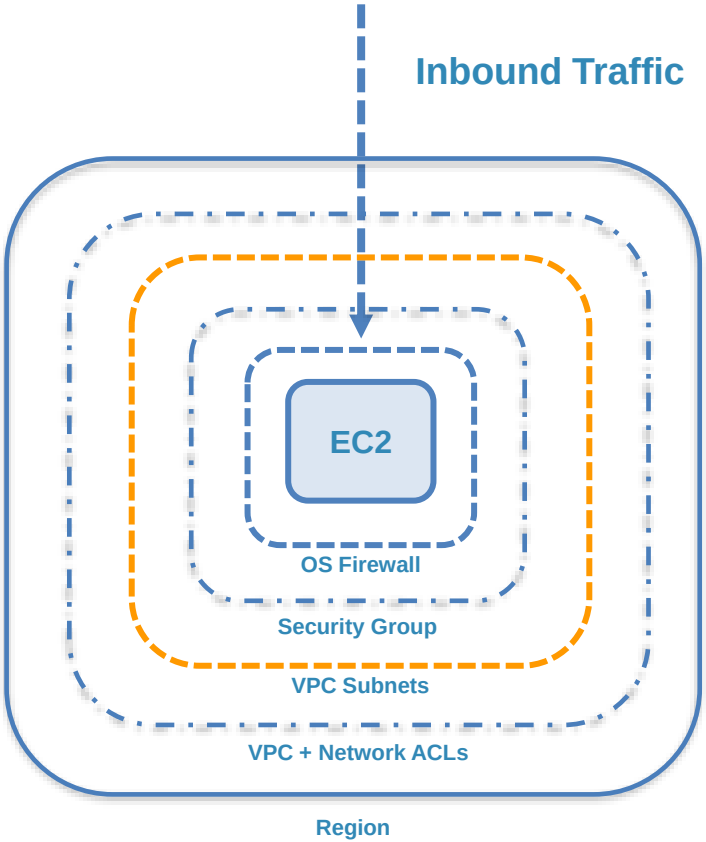
Well-Architected Partners

https://aws.amazon.com/architecture/well-architected/partners/

aws

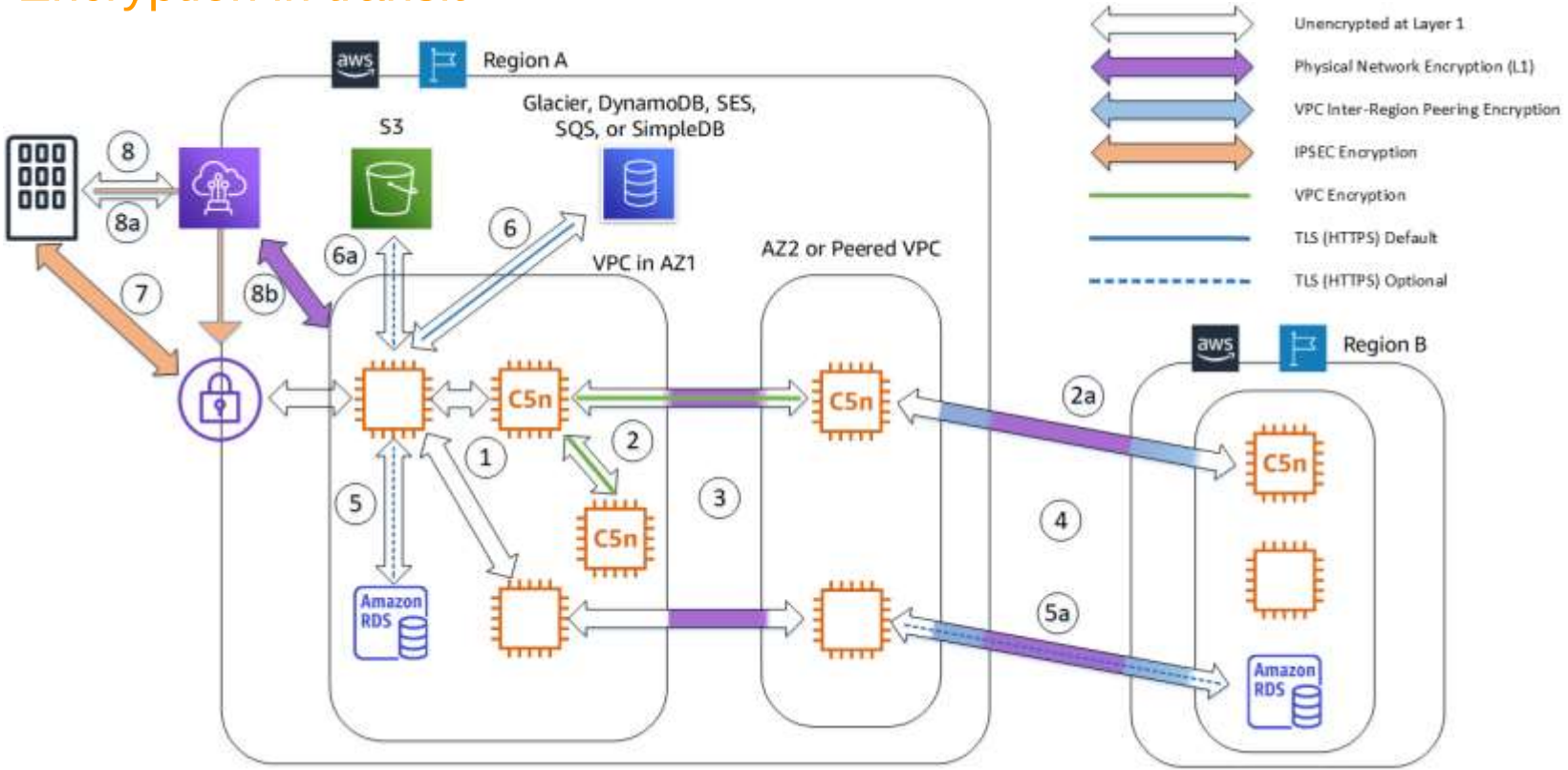
Multi-dimensionaler “Defense in depth”

- Infrastruktur als Code
- VPCs
- Private und öffentliche Subnetze
- Sicherheitsgruppe und ACLs
- Jede Instanz ist durch eine Stateful Firewall geschützt
- NACL (zustandslose Regeln, zweite Schutzstufe auf Netzwerkebene)
- Private Konnektivität zur lokalen Umgebung

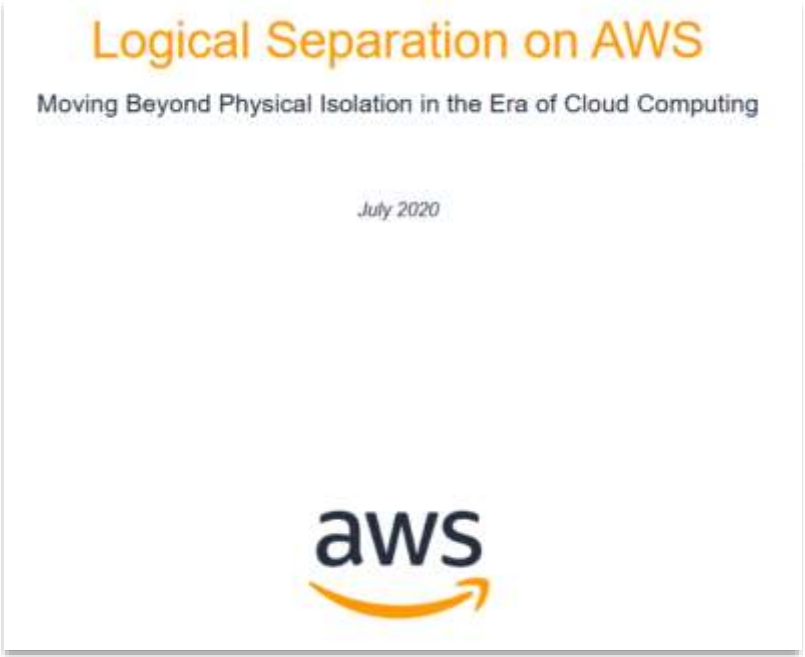


https://docs.aws.amazon.com/whitepapers/latest/logical-separation/logical-separation.pdf

Encryption in transit



Logische Trennung



mehrgliederiger Ansatz:

- Authentisierung und Autorisierung
- Virtualisierung
- Verschlüsselung
- Monitoring und Logging
- Bereitstellen von Computing auf dedizierter Hardware
- Serverless und Container

Kombiniert mit Sichtbarkeit & Kontrolle bieten APIs die Möglichkeit vertrauliche Workloads sicher in die Cloud zu migrieren, ohne dass eine physisch dedizierte Infrastruktur erforderlich ist.

https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf
https://pages.awscloud.com/aws-webinar-on-demand-cloud-security-essentials-thank-you.html

Linksammlung

Sichere Verwaltung des Zugriffs auf Services und Ressourcen	AWS Identity and Access Management (IAM)
Single Sign-On (SSO)-Service für die Cloud	AWS Single Sign-On
Identitätsverwaltung für Ihre Apps	Amazon Cognito
Verwaltetes Microsoft Active Directory	AWS Directory Service
Einfacher und sicherer Service zum Teilen von AWS-Ressourcen	AWS Resource Access Manager
Zentrale Steuerung und Verwaltung über AWS-Konten hinweg	AWS Organizations
Einheitliches Sicherheits- und Compliance-Zentrum	AWS Security Hub
Verwalteter Service zur Bedrohungserkennung	Amazon GuardDuty
Analysieren der Anwendungssicherheit	Amazon Inspector
Aufzeichnen und Beurteilen der Konfigurationen Ihrer AWS-Ressourcen	AWS Config
Nachverfolgen der Benutzeraktivität und API-Nutzung	AWS CloudTrail
Sicherheitsverwaltung für IoT-Geräte	AWS IoT Device Defender
DDoS-Schutz	AWS Shield
Filtern von bösartigem Web-Datenverkehr	AWS-Firewall für Webanwendungen (FWA)
Zentrale Verwaltung von Firewallregeln	AWS Firewall Manager
Erkennen und Schützen von vertraulichen Daten beliebigen Umfangs	Amazon Macie
Schlüsselspeicherung und -verwaltung	AWS Key Management Service (KMS)
Hardwarebasierter Schlüsselspeicher für Einhaltung von Vorschriften	AWS CloudHSM
Öffentliche und private SSL-/TLS-Zertifikate bereitstellen und verwalten	AWS Certificate Manager
Rotieren, Verwalten und Abrufen von Secrets	AWS Secrets Manager
Untersuchen potenzieller Sicherheitsprobleme	Amazon Detective
Schnelle, automatisierte und kostengünstige Notfallwiederherstellung	CloudEndure Disaster Recovery

Kostenloses Self-Service-Portal für bedarfsorientierten Abruf von AWS Compliance-Berichten AWS Artifact

https://aws.amazon.com/de/products/security/

aws

Linksammlung

Handbücher und API-Referenzen
Overview of Security Processes
AWS Global Infrastructure
Managing Security on AWS
AWS Well-Architected – Security
Security Pillar AWS Well Architected Framework

Berlin Summit AWS Security - Stephen Schmidt CISO
AWS network and infrastructure security (Deloitte)

AWS Security Hub
AWS Provable Security
AWS Data Center
AWS Security Documentation
AWS Cloud Security
AWS Compliance
AWS Compliance Center
Testimonials For Security and Compliance
Conformance-Packs

AWS Data Privacy
AWS Data Privacy FAQ
AWS Datenschutz Whitepaper
GDPR Center
Navigating GDPR Compliance on AWS
Data Classification
Data Residency
EUGH Privacy Shield und Standardvertragsklauseln
Pseudonymisieurungslösungen

Risk and Compliance
Resilience
Resilience Testing

SANS Practical Guide to Security in the AWS Cloud
Open Government Solutions

Videosammlung

AWS re:Inforce 2019: How Encryption Works in AWS (FND310-R)

The Nitro Project - Next-Generation EC2 Infrastructure

AWS re:Inforce 2019: Security Benefits of the Nitro Architecture (SEP401-R)
AWS re:Invent 2022 – Confidential Computing with AWS compute (CMP302)

Security und Compliance: Grundlagen und Best Practices für die Public Cloud - post SchremsII

Techtalk 1 Datensicherheit in der Cloud
Techtalk 2 Wie kann ich meine Daten technisch sicher in der Cloud speichern?

From Zero to BSI C5: How a small company achieved BSI C5 attestation and how you can do it, too

To learn more about post-quantum cryptography watch the Cryptography in the Next Cycle session from re:Inforce 2019 https://www.youtube.com/watch?v=iBUReOA8s7Y .

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung17 erstellen.
b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria Catalogue – C5 (Kriterienkatalog Cloud Computing) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.18
c) Die Einrichtung MUSS - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) erfüllt.
b) Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.
c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5 verwendet werden. …

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

…

i) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder diese Risiken tragen.

j) Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.

k) Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

…

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.

ii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) die Prüfrechte wahrnehmen können.

…

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

…

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

iii) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

iv) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.
b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.
c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder. Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.
b) Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteerbringer mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

aws

Wissenschaftliche Dienste

Deutscher Bundestag

Ausarbeitung

DSGVO und Nutzung US-amerikanischer Cloud-Dienste

https://www.bundestag.de/resource/blob/852984/692120a134f9e79999c6f4170a47859a/WD-3-102-21-pdf-data.pdf

Auch IP-Adressen sind potentiell personenbezogen, soweit der Provider sie einem Benutzer zuordnen kann und dieses Zusatzwissen des Providers für andere (juristische) Personen zugänglich und erreichbar ist.

Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition
Stand: 1. Februar 2021, Art. 4 DSGVO Rn. 1

https://www.bundestag.de/resource/blob/852984/692120a134f9e79999c6f4170a47859a/WD-3-102-21-pdf-data.pdf

2.2.3. Zur Erfüllung einer rechtlichen Verpflichtung, Art. 6 Abs. 1 S. 1 lit. c) DSGVO

Gemäß Art. 6 Abs. 1 S. 1 lit. c) DSGVO dürfen Daten verarbeitet werden, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Art. 6 Abs. 3 S. 2 DSGVO präzisiert, dass **als Rechtsgrundlage nur Unionsrecht** oder das **nationale Recht** der **Mitgliedstaaten** in Betracht kommt. Ein US-amerikanischer Cloud-Anbieter mit Niederlassung in der EU könnte sich daher nicht auf eine mögliche rechtliche Verpflichtung aus US-Recht berufen.

2.2.4. Allgemeine Interessensabwägung, Art. 6 Abs. 1 S. 1 lit. f) DSGVO

Schließlich kommt der Erlaubnistatbestand der **allgemeinen Interessenabwägung** des Art. 6 Abs. 1 S. 1 lit. f) DSGVO in Betracht. Dafür muss die Übermittlung der Daten zur Wahrung der **berechtigten Interessen des Verantwortlichen** erforderlich sein, wobei die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen dürfen. Ob ein berechtigtes Interesse vorliegt, ist rein normativ zu entscheiden. Dafür wird zunächst der Zweck der Verarbeitung ermittelt und beurteilt. Dadurch, dass Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO einen Ausgleich zwischen den Interessen des Betroffenen und denen des Verantwortlichen schaffen möchte, werden nicht nur rechtliche Interessen berücksichtigt. Vielmehr können **auch wirtschaftliche oder ideelle Interessen** Beachtung finden. Ein berechtigtes Interesse kommt daher in Betracht, wenn die Verwaltung aus Kostengründen auf Speicherplatz in einer Cloud zurückgreifen will. In einem zweiten Schritt ist dieses berechtige Interesse mit den Interessen und Grundrechten und Grundfreiheiten des Betroffenen **abzuwiegen**. Als schutzwürdige Interessen der betroffenen Personen sind deren allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 Grundgesetz (GG)) sowie das Recht auf den Schutz personenbezogener Daten (Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh)) zu berücksichtigen. Das Ergebnis der Abwägung hängt dabei vom jeweiligen Einzelfall ab.

3. Fazit

Ein Transfer personenbezogener Daten im Zusammenhang mit Cloud-Computing an ei nur unter den besonderen Voraussetzungen der Art. 44 ff. DSGVO zulässig. Seit dem sog. Schrems II-Urteil des EUGH ist es nicht mehr möglich, die Übermittlung auf einen Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO zu stützen. Eine Übermittlung auf der Grundlage von geeigneten Garantien nach Art. 46 DSGVO, wie beispielsweise Standarddatenschutzklauseln oder Binding Corporate Rules, bleibt grundsätzlich möglich. In diesem Fall müssen aber zusätzliche Maßnahmen getroffen werden, die die übermittelten Daten im konkreten Einzelfall angemessen vor dem unbeschränkten Zugriff der US-Sicherheitsbehörden schützen. Als zusätzliche Maßnahmen kommen insbesondere verschiedene Formen der Datenverschlüsselung in Betracht. Diese werden jedoch nicht in jedem Fall praktikabel oder ausreichend sein. Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er verpflichtet, die Übermittlung personenbezogener Daten in die USA auszusetzen oder zu beenden. Neben den geeigneten Garantien des Art. 46 DSGVO besteht die Möglichkeit der Datenübermittlung nach einem der in Art. 49 DSGVO normierten Ausnahmetatbestände. Diese sind jedoch eng auszulegen, da das von der DSGVO vorgesehene Regel-Ausnahmeverhältnis nicht missachtet werden darf. Zudem bestehen Zweifel an der Praktikabilität des Ausnahmetatbestandes der Einwilligung, die hier am ehesten in Betracht zu ziehen sein dürfte.