AWS
TRANSFORMATION DAY
GERMANY

Data Protection in the AWS Cloud: Implementing GDPR and Overview of C5

Gerald Boyne, Christian Hesse
Security Assurance Germany
25.11.2017

aws

Agenda

- Basics on GDPR
- Navigating GDPR Compliance on AWS
- Cloud Computing Compliance Controls Catalogue (C5)
- Conclusion

Basics on GDPR

Title + Content

- Will come into effect 25.05.2018
- Follows EU Data Protection Directive (Directive 95/46/EC)
- Regulation vs. Directive

Basics on GDPR

- It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.
- High penalties
- PII data transfers to countries outside the EU with high hurdles
- Right to data portability
- Right to be forgotten
- Privacy by design
- Data breach notification within 72 hours to authorities

Data protection is a shared responsibility

DPA, Consent etc.

Data Subject

Data Controller

Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

DPA, EU SCC

AWS Foundation Services

Compute

Storage

Database

Networking

aws

AWS Global Infrastructure

Availability Zones

Regions

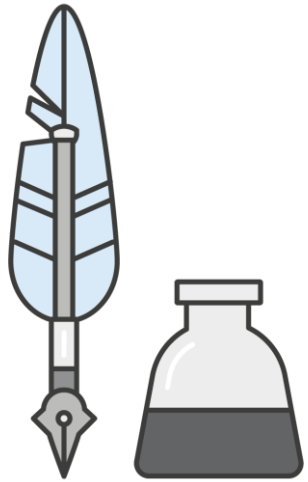
Edge Locations

Data (Sub) processor

aws

Data Processing Agreement/Addendum

- AWS has a GDPR-ready DPA available for customers today that is effective 25 May 2018. If applicable, any existing EU General Data Protection Directive DPA becomes invalid at midnight, 24 May 2018.
- Work with your AWS account team to obtain the AWS GDPR Data Processing Addendum.



Navigating GDPR Compliance on AWS

Scope/Purpose

1. Decide what to do (Strategy)

1.1 Identify Stakeholders

1.2 Identify Your Workloads Moving to AWS

Privacy by Design

2. Analyze and Document (outside of AWS)

2.1 Rationalize Security Requirements

2.2 Define Data Protection Controls

2.3 Document Security Architecture

Monitoring of processing activities

3. Automate, Deploy & Monitor

3.1 Build/deploy Security Architecture

3.2 Automate Security Operations

3.3 Continuous Monitor

3.4 Testing and Game Days

Strong Compliance Framework and Security Standards

4. Certify

4.1 Audit and Certification

aws

Navigating GDPR Compliance on AWS (examples)

GDPR Art. 17: Data Portability

Network Connections, APIs, Snowball

GDPR Art. 32: Encryption

Encryption

Key Management Service

CloudHSM

Server-side Encryption

GDPR Art. 25: Data Access Control

Identity

IAM

Active Directory Integration

SAML Federation

GDPR Art. 17/30: Monitoring of processing

Compliance

Service Catalog

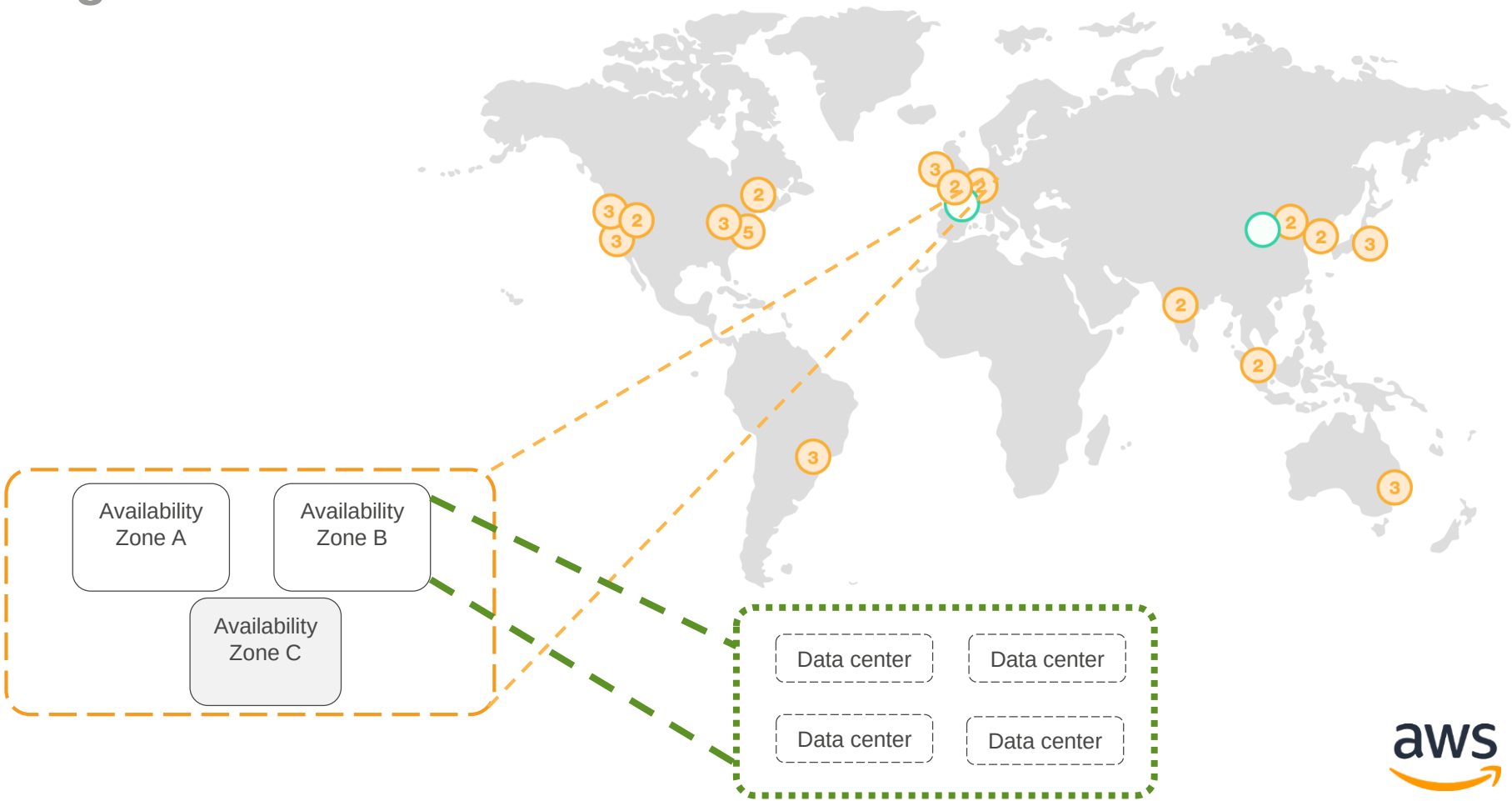
CloudTrail

Config

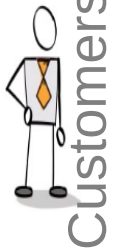
aws

Cloud Computing Compliance Controls Catalogue (C5)

Region – Frankfurt



Shared Responsibility Model



Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

- ✓ *AWS Best Practices*
- ✓ *Industry Standards*
- ✓ *AWS Architecture for Standards*
- ✓ *Internal & Regulatory Requirements*
- ✓ *Service Documentation*
- ✓ *AWS Workbooks*
- ✓ *AWS Technology Resources*

AWS Foundation Services

Compute | **Storage** | **Database** | **Networking**

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

AWS Agreements

C5 = Cloud Computing Compliance Controls Catalogue

Designed and released by the BSI in February 2016, the C5 control set offers additional assurance to customers in Germany as they move their complex and regulated workloads to Cloud Computing Service providers such as AWS.

The following international standards had been taken by BSI into account:

- **ISO/IEC 27001:2013** (ISO - International Organization for Standardization)
- **CSA Cloud Controls Matrix 3.01** (CSA - Cloud Security Alliance)
- **AICPA Trust Service Principles Criteria 2014** (AICPA - American Institute of Certified Public Accountants)
- **ANSSI Référentiel Secure Cloud 2.0 (Draft)** (ANSSI - Agence nationale de la sécurité des systèmes d'information)
- **IDW ERS FAIT 5 04.11.201** (draft of a statement on accounting: "Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing" [Generally accepted accounting principles for the outsourcing of accounting-related services including cloud computing], version of 4 November 2014)
- **BSI IT-Grundschutz Catalogues**, 14th version 2014•
- **BSI SaaS Sicherheitsprofile 2014** [BSI SaaS security profiles 2014]

Mapping table https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/Referencing_Cloud_Computing_Compliance_Controls_Catalogue.pdf

Dr. Patrick Grete, Project lead C5 at BSI

mentions additional advantages: „A novelty of C5 in respect to other security standards are the so called **surrounding parameters**.

They deliver information concerning

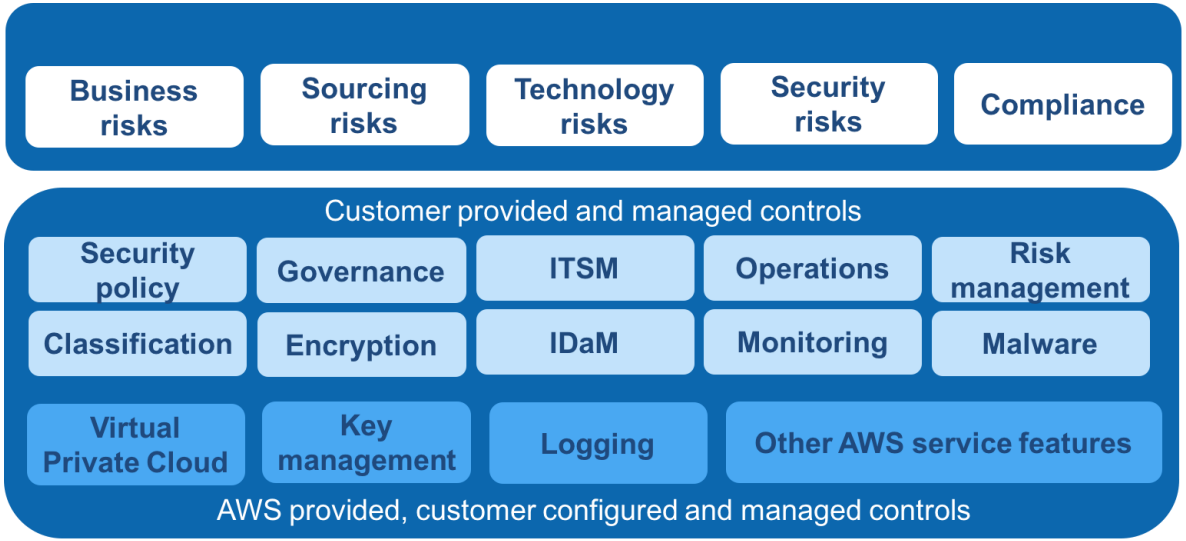
- **data location**
- **service provisioning**
- **place of jurisdiction**
- **existing certifications**
- **and obligation duties for inquiries and revelation towards public authorities**
- **and contain a system description**

The thereby generated transparency allows a customer to decide if legal regulations (as i.e. data privacy), own company policies or the threat situation of industrial espionage makes it reasonable to use a specific cloud service.“

Mapping table https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/Referencing_Cloud_Computing_Compliance_Controls_Catalogue.pdf

Governance in the Cloud

Customers decide on the appropriate controls and processes to manage and monitor the effectiveness of those controls



Based on Customers' Controls, Customer identifies and documents controls operated by AWS

AWS TRANSFORMATION DAY GERMANY

Additional Ressources:

http://aws.amazon.com/documentation
http://aws.amazon.com/compliance
http://aws.amazon.com/security