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

Gerald Boyne, Christian Hesse
Security Assurance Germany
25.11.2017
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.
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
Navigating GDPR Compliance on AWS (examples)

<table>
<thead>
<tr>
<th>GDPR Art. 17: Data Portability</th>
<th>GDPR Art. 32: Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Connections, APIs, Snowball</td>
<td>Encryption</td>
</tr>
<tr>
<td>Key Management Service</td>
<td>CloudHSM</td>
</tr>
<tr>
<td>Server-side Encryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GDPR Art. 25: Data Access Control</th>
<th>GDPR Art. 17/30: Monitoring of processing</th>
<th>GDPR Art. 17: Data Portability</th>
<th>GDPR Art. 32: Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>Identity</td>
<td>Identity</td>
<td>Encryption</td>
</tr>
<tr>
<td>Active Directory Integration</td>
<td>SAML Federation</td>
<td>SAML Federation</td>
<td>CloudHSM</td>
</tr>
<tr>
<td>SAML Federation</td>
<td>Compliance</td>
<td>Compliance</td>
<td>Service Catalog</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>Config</td>
<td>Config</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Computing Compliance Controls Catalogue (C5)
Region – Frankfurt

Availability Zone A

Availability Zone B

Availability Zone C

Data center

Data center

Data center

Data center
**Shared Responsibility Model**

**AWS Foundation Services**
- Compute
- Storage
- Database
- Networking

**AWS Global Infrastructure**
- Availability Zones
- Regions
- Edge Locations

**Customer content**
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall Configuration
- Client-side Data Encryption
- Server-side Data Encryption
- Network Traffic Protection

- AWS Agreements

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

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.“

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 managed and audited controls**

- SOC 1
- SOC 2
- C5
- ISO 27001
- ISO 27017
Additional Ressources:

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