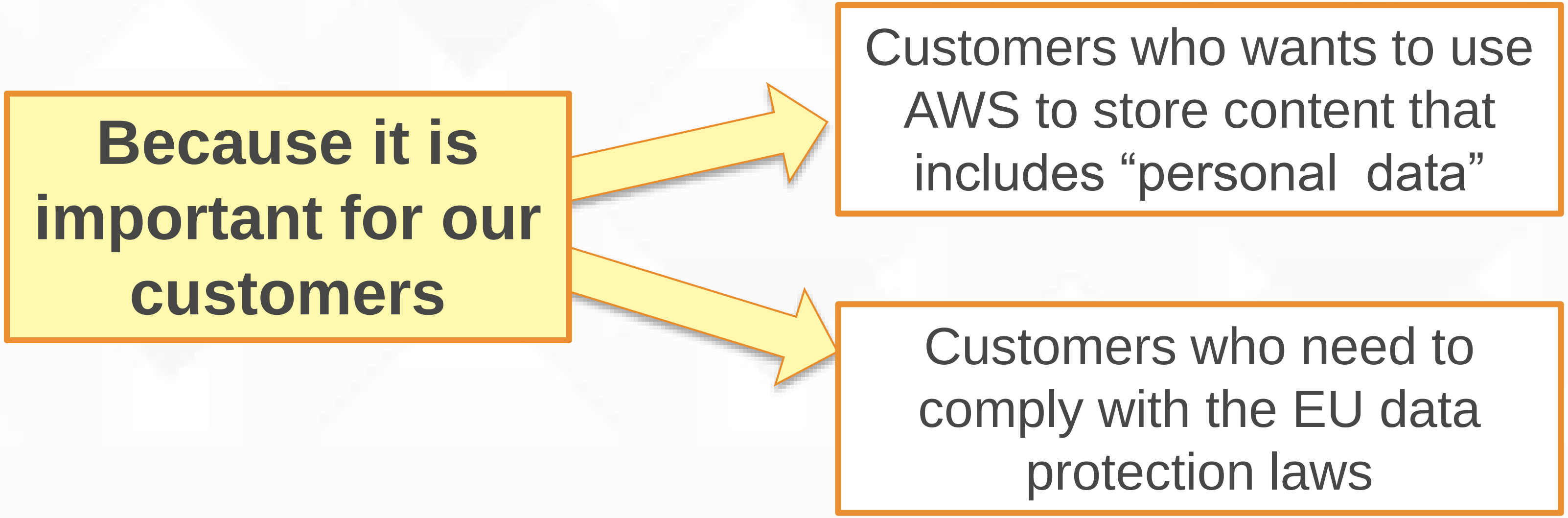
AWS Summit

Berlin

Introduction to AWS
Data Protection White Paper

Nadia Meliti, AWS Legal

Why a White Paper?



Because it is important for our customers

Customers who wants to use AWS to store content that includes “personal data”

Customers who need to comply with the EU data protection laws

What are these laws?

- ❑ **Data Protection Directive 1995**
  - ▪ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  - ▪ Aims to guarantee individual privacy by creating minimum standards
- ❑ **Implemented by EU member states through national laws.**
  - ▪ In 2001, Germany adopted The Federal Data Protection Act or Bundesdatenschutzgesetz (BDSG)

The Directive

- ❑ **Applies when “personal data” is being “processed”.**
  - “Personal data” is information from which a living individual may be identified or identifiable (known as the “data subject”).
  - “Processing” includes any operation or set of operations which is performed upon personal data.
- ❑ **Distinguishes between**
  - “Data controller” - has primary responsibility for legal compliance
  - “Data processor” – must follow controller’s instructions

What is Customer’s Role?

❑ Customer is a “controller” if

- it determines the purpose for which the data will be processed and determines how it will be processed.

❑ Customer will be a “processor” if

- it is merely processing the personal data on behalf of and according to the wishes of a third party.

AWS Services

- ❑ Customers using AWS can decide:
  - What content to upload onto the AWS network
  - Whether or not it will be personal data
  - How the content will be processed
  - Where it will be located (e.g. type of storage and geographic location)
  - The format of the content (e.g. plain text, masked, anonymised or encrypted, using either AWS provided encryption or a third-party encryption mechanism of the customer’s choice)
  - If / how the content will be protected (e.g. by using access controls)

What is AWS’ Role?

- ❑ **Customers determine if AWS will be a data processor**
  - ▪ If customer decides to upload personal data on AWS, then AWS is processing personal data.

- ❑ AWS services are automated and self-service

- ❑ As a provider of IaaS, AWS:
  - ▪ does not know what content the customers are choosing to store on AWS
  - ▪ cannot distinguish between personal data and other content

What are the legal requirements?

Data controllers must ensure that data processing will comply with the following principles:

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. Data retention
7. Data security
8. Data transfers

Key Principles

1. **Fairness**
2. Lawful basis
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. Data retention
7. Data security
8. Data transfers

- Data subjects must get all details to guarantee fair processing.
- Customer (or its customer) decides what data is collected and why.
- AWS has no visibility of or control over what content customer chooses to store on AWS and why.

Key Principles

1. Fairness
2. **Lawful basis**
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. Data retention
7. Data security
8. Data transfers

- Customer (or its customer) must have lawful basis for processing data and satisfy at least one legal criteria - e.g. by getting data subject’s consent.

- AWS cannot ascertain whether there is a lawful basis for processing data or provide for it.

Key Principles

1. Fairness
2. Lawful basis
3. **Purpose Limitation**
4. Data subject rights
5. Accuracy
6. Data retention
7. Data security
8. Data transfers

❖ Customer (or its customer) must have a specified, explicit and legitimate purpose for collecting and processing personal data.

❖ AWS has no visibility of or control over purposes for which customer uses its content on AWS.

❖ AWS only processes the content to provide to the customer those AWS services selected by that customer.

Key Principles

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. **Data subject rights**
5. Accuracy
6. Data retention
7. Data security
8. Data transfers

- ❖ Data subjects need access to their personal data, and rectification, erasure or blocking of it if processed inappropriately.
- ❖ Customer retains control of data stored on AWS; it can accommodate data subjects access/other rights.
- ❖ AWS does not access customer's content except to provide customer with services; AWS cannot connect content stored on AWS with any particular person.

amazon web services

Key Principles

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. Data subject righ
5. **Accuracy**
6. Data retention
7. Data security
8. Data transfers

❖ Customer (or its customer) must ensure that personal data is accurate and kept up to date.

❖ AWS does not enter or modify any personal data on customers' behalf. AWS is unable to verify or maintain the accuracy of customer's content or to update it.

Key Principles

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. **Data retention**
7. Data security
8. Data transfers

❖ Personal data cannot be kept in an identifiable form longer than necessary for the purposes for which it was collected.

❖ Customer (or its customer) decides purposes for the data it stores on AWS and for how long to retain it.

❖ AWS has no insight into customer’s purposes or how long content must be retained to achieve these purposes.

Key Principles

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. Data retention
7. **Data security**
8. Data transfers

- Appropriate technical and organizational measures (“TOM’s”) must be implemented to protect data.

- Customer is in the best position to determine which TOM’s are appropriate and to implement them to protect data it uploads on AWS.

TOM’s in the Cloud context

❑ Unlike traditional hosting solutions

- AWS provides customers with a selection of optional security measures
- Customers can also choose from variety of third party security solutions

❑ Here customer is empowered to:

- decide if it wants to implement security measures to protect its content
- determine which TOM’s are appropriate to implement – no differently than it would in an on-site data center
- design its own security architecture to meet its compliance needs

TOM’s in the Cloud context

❑ Security *IN* the cloud

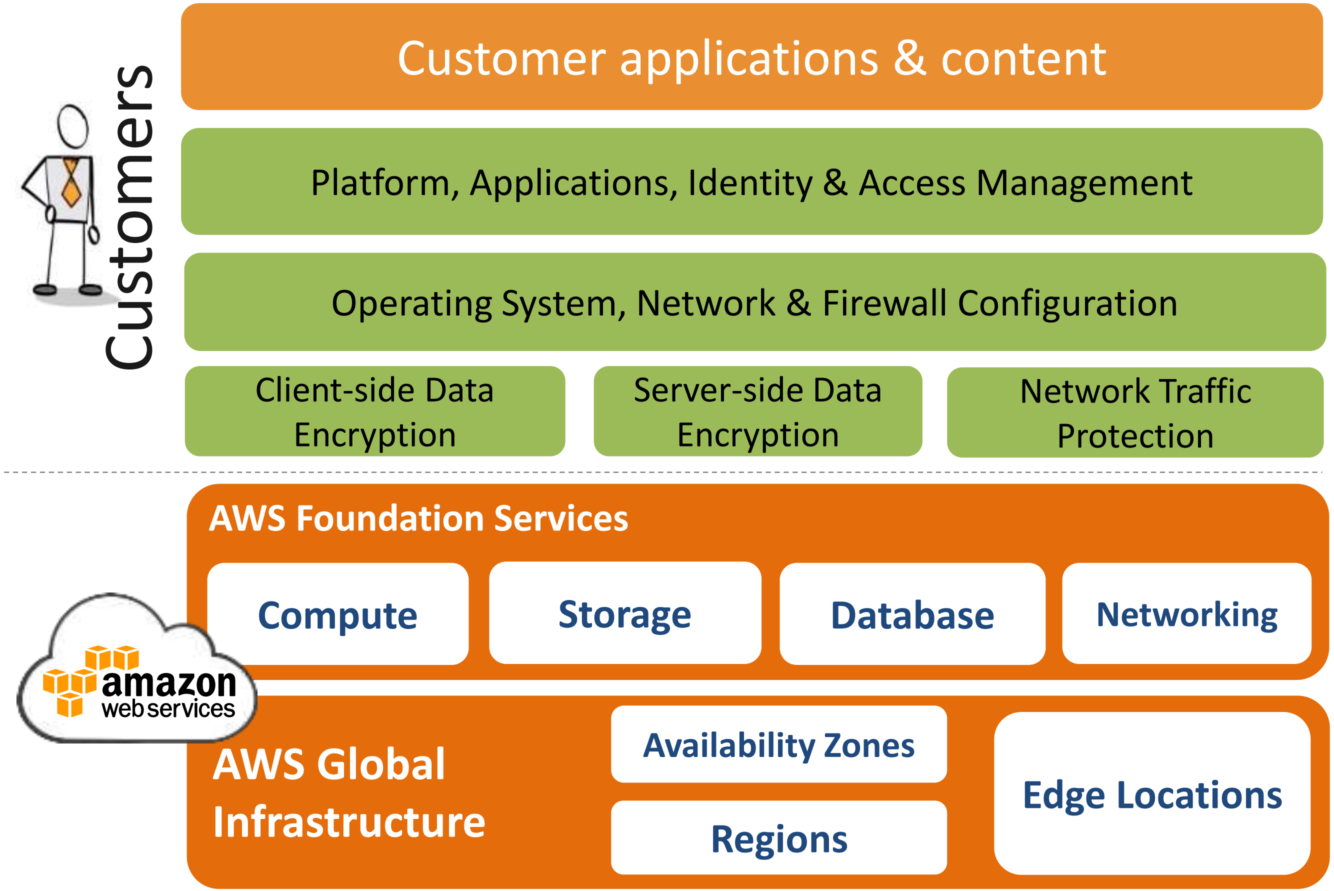
Customers are responsible for:

- configuring the AWS services properly
- Implementing appropriate security controls and backup
  - E.g. by using encryption and routine archiving.

❑ Security *OF* the cloud

AWS is responsible for security of the underlying cloud

Security & compliance is a shared responsibility



Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Customers are responsible for their security **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

Key Principles

1. Fairness
2. Lawful basis
3. Purpose Limitation
4. Data subject rights
5. Accuracy
6. Data retention
7. Data security
8. **Data transfers**

- Personal data may not be transferred outside EEA without adequate protection.

- Customer chooses where location of its content. Customer can choose to deploy their AWS services exclusively in the AWS EU Regions in Germany or Ireland.

- AWS does not move customer content outside of the customer’s chosen Region(s) unless required by law.

Data Sovereignty

❑ Depending on where customers (or their customers) are doing business, laws in other jurisdictions may apply

❑ Broadly speaking:

- Many EU Member States' laws enable national security / law enforcement bodies to seek access to information
- Law enforcement bodies can use recognized international processes – e.g. Mutual Legal Assistance Treaties

❑ AWS Policy

- AWS will not disclose customer content unless required to comply with a legally valid and binding order
- We carefully examine each request to authenticate its accuracy and verify that it complies with law
- We will challenge requests that are overbroad, exceed requestor's authority or do not fully comply with law.
- We notify customers to allow them to seek protection from disclosure, unless prohibited by law

Customer’s Compliance Toolkit

❑ AWS can offer customers:

- Many tools, including independent validations, certifications, white papers
- a data processing agreement (“DPA”)
- US Safe Harbor certification
- Standard EU Contractual Terms (“Model Clauses”)

❑ Article 29 Working Party approved our DPA, including the Model Clauses:

- Customer can now rely on our terms to enable compliant data flows
- For more detail, please visit the Luxembourg Data Protection Authority webpage:

http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Where to find out more?

❑ Visit our website and download the EU Data Protection White Paper:

http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf

Thank You

amazon
web services