



AWS Webinar

Navigating GDPR Compliance on AWS

Christian Hesse
Amazon Web Services





What is the GDPR?





What is the GDPR?

- The "GDPR" is the General Data Protection Regulation, a significant new EU Data Protection Regulation
- Introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance across the EU
- The GDPR is enforceable **May 25th, 2018** and it replaces the EU Data Protection Directive (Directive 95/46/EC)
- Territorial scope: Organisations established in the EU and Organisations without an EU presence who target or monitor EU individuals

Content vs. Personal Data

Content

= anything that a customer (or any end user) stores, or processes using AWS services, including:

Software | Data | Text | Audio | Video

Personal Data

= information from which a living individual may be ***identified*** or ***identifiable*** (under EU data protection law)

- Customer's "content" might include "personal data"



What Else Comes With GDPR?

**The Right to Data
Portability**

**The Right to Be
Forgotten**

**Privacy By
Design**

**Data Breach
Notification**

Individuals have the right to a copy of all the personal data that **controllers** have regarding him or her. It also must be provided in a way that facilitates reuse.



What Else Comes With GDPR?



**The Right to Data
Portability**

**The Right to Be
Forgotten**

**Privacy By
Design**

**Data Breach
Notification**

This gives individuals the right to have certain personal data deleted so third parties can no longer trace them.





What Else Comes With GDPR?

**The Right to Data
Portability**

**The Right to Be
Forgotten**

**Privacy by
Design**

**Data Breach
Notification**

This helps to facilitate the inclusion of policies, guidelines, and work instructions related to data protection in the earliest stages of projects including personal data.



What Else Comes With GDPR?



**The Right to Data
Portability**

**The Right to Be
Forgotten**

**Privacy By
Design**

**Data Breach
Notification**

Controllers must report personal data breaches to the relevant supervisory authority within 72 hours. If there is a high risk to the rights and freedoms of data subjects, they must also notify the data subjects.





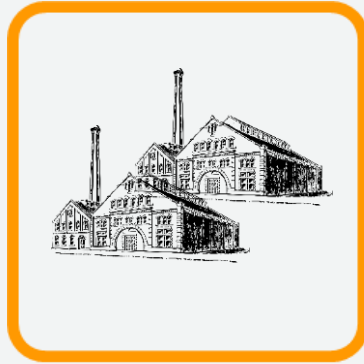
How AWS can help customers achieve GDPR compliance



Bringing it all together



Data Subjects



**Customers are
Controllers**



**AWS as
Processor**

**Controllers and Processors have
obligations under GDPR**

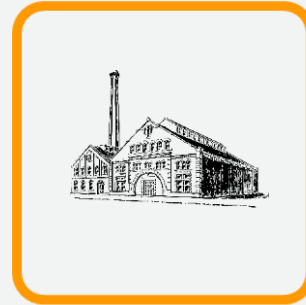
Bringing it all together



Data Subjects



Customer's customer
as Controller



Customer as
Processor



AWS as Processor

**Controllers and Processors have
obligations under GDPR**

GDPR in practice: implementing TOMs



Under GDPR **Controllers** and **Processors** are required to implement appropriate Technical and Organization Measures (“TOMs”) ...

(1) Pseudonymisation and encryption of personal data

(2) Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services

(3) Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident

(4) Process for regularly testing, assessing, and evaluating the effectiveness of TOMs



What AWS provides



Tools and Services



Compliance Framework

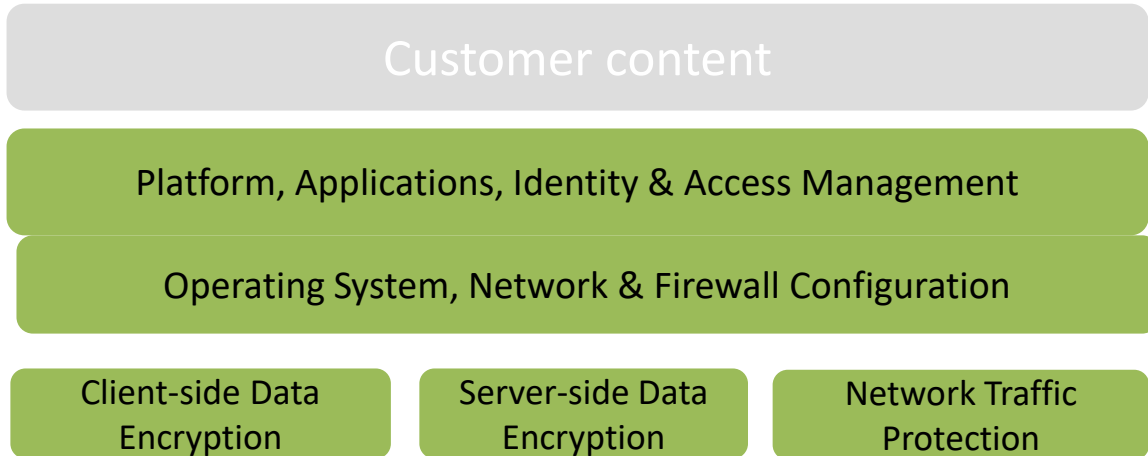


Partner Network



Data Protection Terms

AWS Shared Responsibility Model

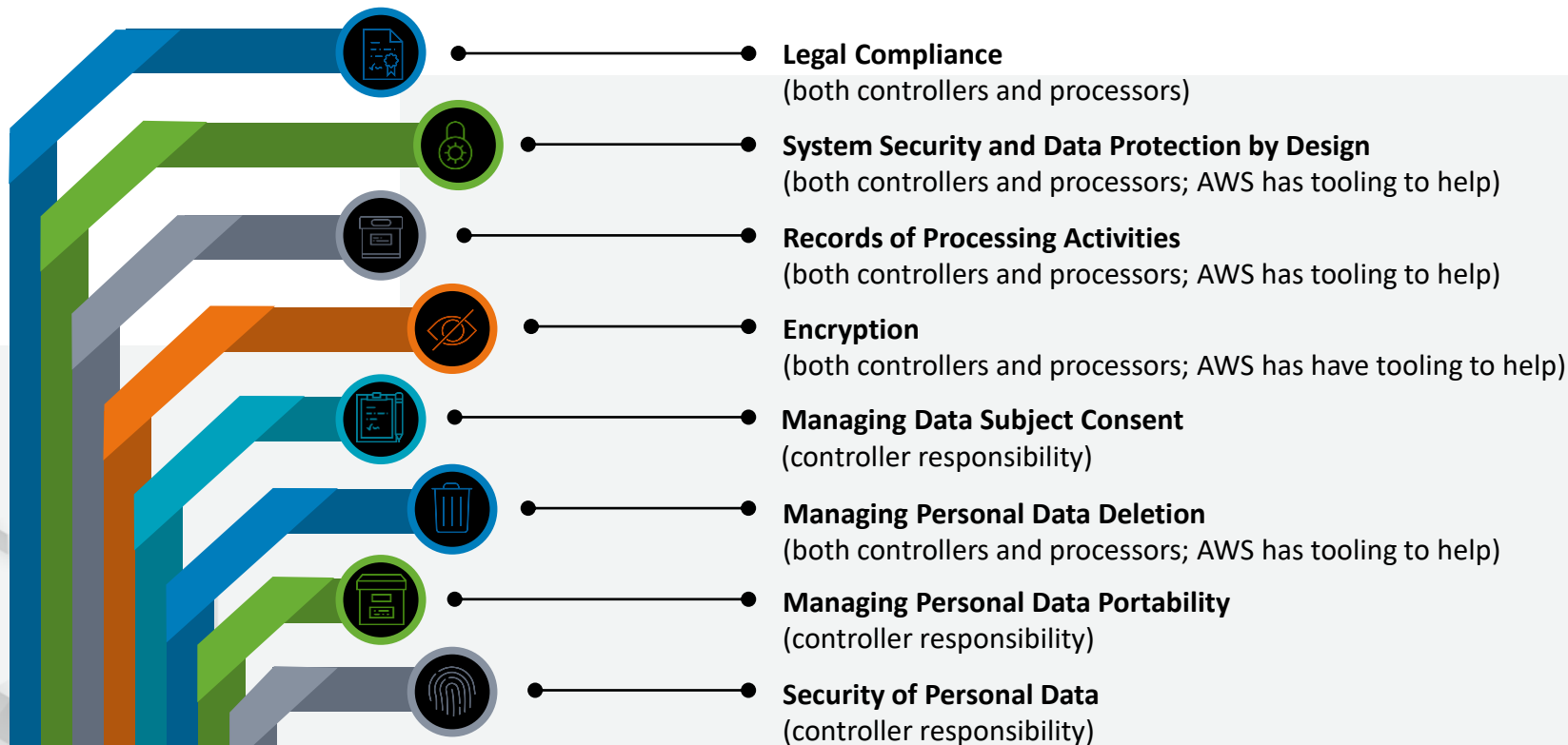


Customers are responsible for their security and compliance **IN** the Cloud



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

GDPR is also a “shared responsibility”



Navigating GDPR Compliance with AWS Services

'Data protection by design and default'



Amazon Snowball



Amazon API Gateway



Amazon Virtual Private Cloud (VPC)



AWS Identity and Access Management



Active Directory Integration



SAML Federation

'Security of processing'



AWS KMS



AWS CloudHSM



Server-side Encryption

'Records of processing activities'



AWS Service Catalog



AWS CloudTrail



AWS Config

GDPR Compliance Tools



**Data Access
Control**

**Monitoring of
Access Activities**

**Data
Encryption**

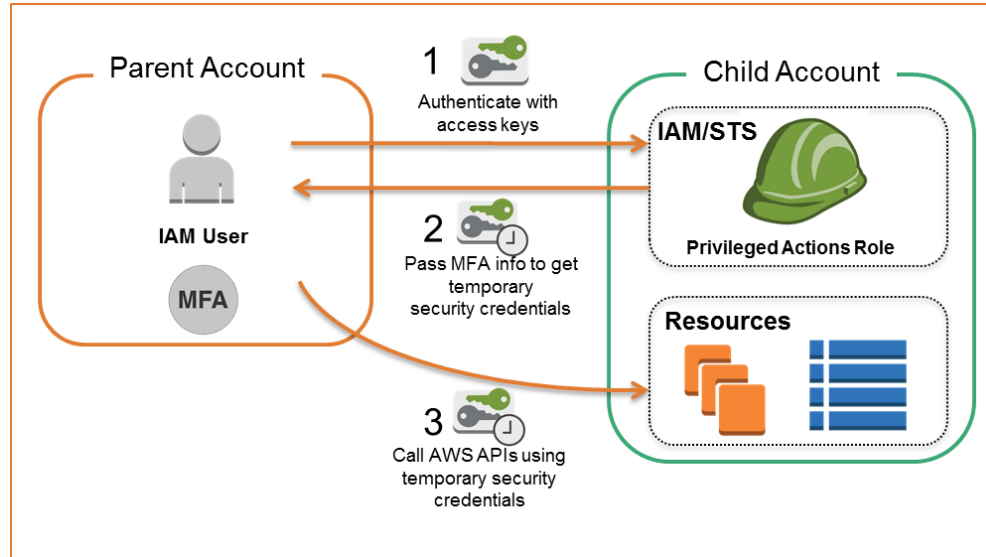
**Strong Compliance
Framework**

The **controller** “shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.”

Multi factor authentication
API-Request Authentication
Temporary Access Tokens

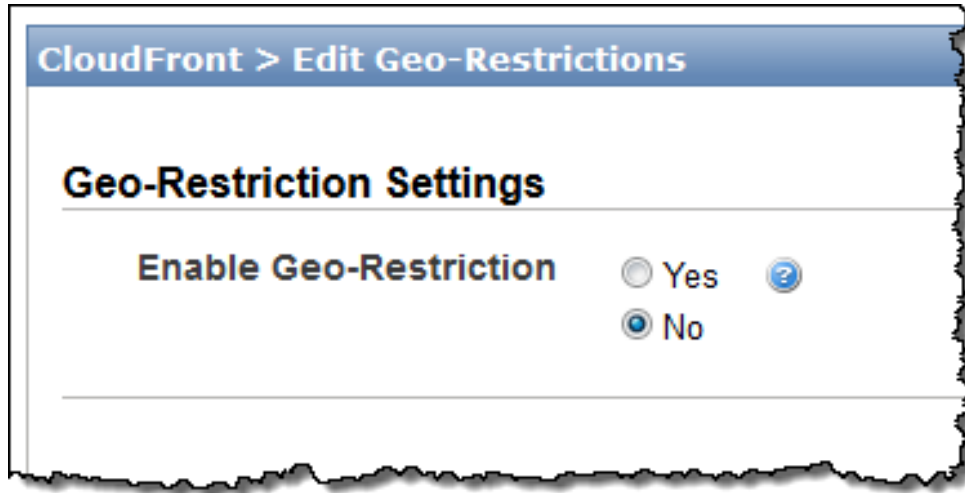
AWS & The GDPR

Access Control



AWS & The GDPR

Access Control



GDPR Compliance Tools



**Data Access
Control**

**Monitoring of
Access Activities**

**Data
Encryption**

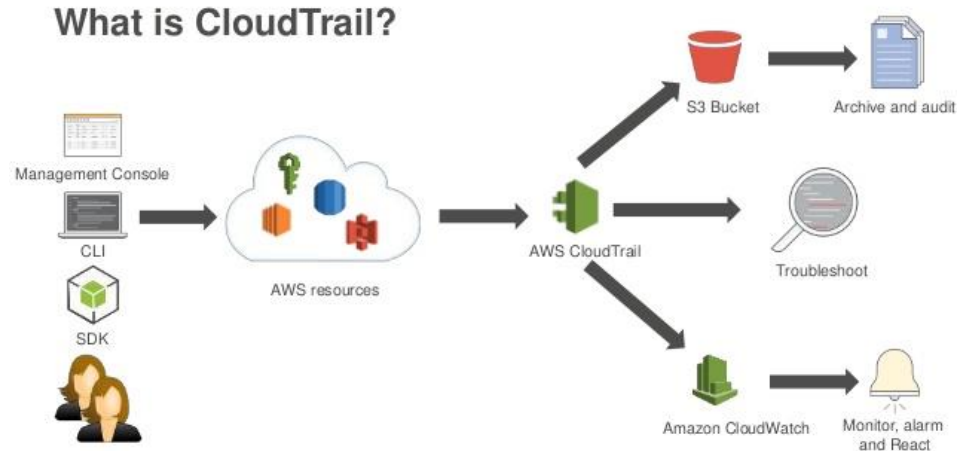
**Strong Compliance
Framework**

“Each **controller** and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.”

CloudTrail
Inspector
Macie
AWS Config

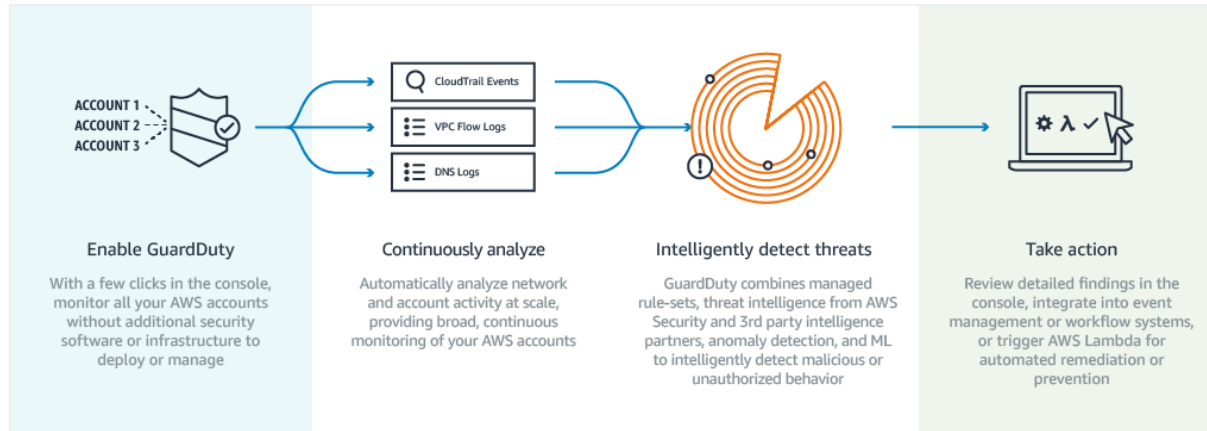
AWS & The GDPR

Monitoring and Logging



AWS & The GDPR

Amazon GuardDuty



GDPR Compliance Tools



**Data Access
Control**

**Monitoring of
Access Activities**

**Data
Encryption**

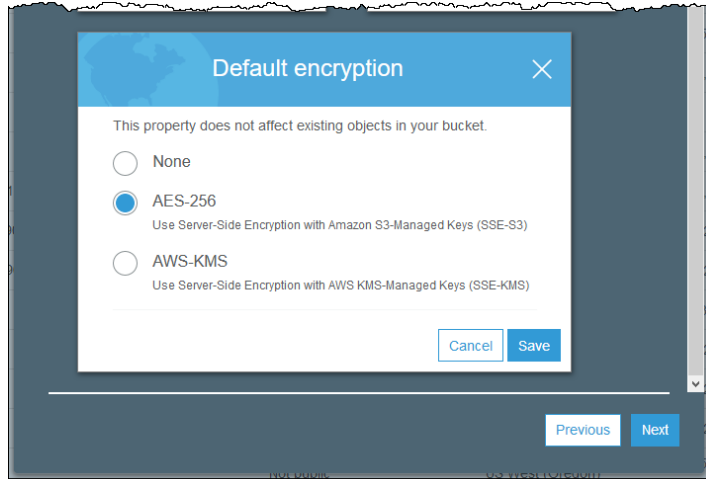
**Strong Compliance
Framework**

Organizations must “implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the pseudonymisation and encryption of personal data.”

Encryption of your data at rest with AES256 (EBS/S3/Glacier/RDS)
Centralized (by Region) managed Key-Management (KMS)
IPsec tunnels into AWS with the VPN-Gateways
Dedicated HSM modules in the cloud with CloudHSM

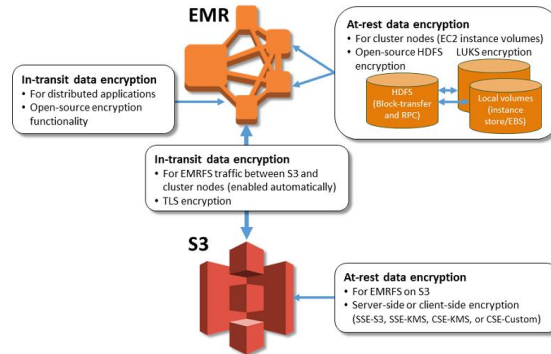
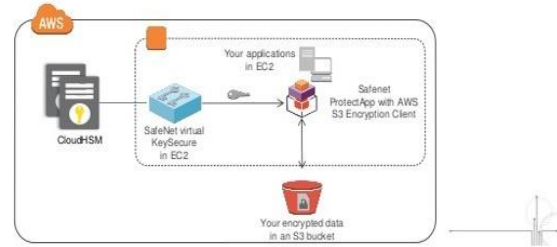
AWS & The GDPR

Encryption



S3 Encryption

Encryption of S3 objects using master keys in CloudHSM



AWS & The GDPR

Amazon Key Management Service (KMS)

SSE using KMS



Keys managed centrally in Amazon KMS with permissions and auditing of usage

GDPR Compliance Tools



**Data Access
Control**

**Monitoring of
Access Activities**

**Data
Encryption**

**Strong Compliance
Framework**

Appropriate technical and organizational measures may need to include “the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services.”

SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70) / SOC 2 / SOC 3

PCI DSS Level 1

ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018

FIPS 140-2

C5

Meet your own security objectives



Customers

Your own accreditation

GDPR
Code of
Conducts

Your own certifications



Your own external audits



Customer scope
and effort is
reduced

Better results
through **focused
efforts**

AWS Foundation Services



AWS Global
Infrastructure



Built on AWS
consistent
baseline controls

GDPR – Codes of Conduct



CISPE Code (Cloud Infrastructure Service Providers in Europe)

The CISPE [Code of Conduct](#) :

- An effective, easily accessed framework for complying with the EU's [GDPR](#)
- Excludes the re-use of customer data
- Enables data storage and processing exclusively within the EU
- Identifies cloud infrastructure services suitable for different types of data processing
- Helps citizens to retain control of their personal and sensitive data
- AWS CISPE certified
- CISPE Code of Conduct in evaluation by Article 29 WP

AWS Marketplace:

One stop shop for **familiar** tools



Advanced Threat Analytics



Application Security



Identity and Access Mgmt



M-Pin SSO
Authentication
for Enterprises

Server & Endpoint Protection



Network Security



Encryption & Key Mgmt



Vulnerability & Pen Testing



AWS Partner Network (APN) & GDPR

Consulting Partners

APN consulting partners can help your customers get ready for GDPR.

Deloitte.

direktgruppe 

sopra  steria

Technology Partners

APN technology partners offer security & identity solutions to help with GDPR.

 BigID

FORTINET



evident.io

ProServe Offering Development: Technical Solution supporting Privacy-by-Design

- SRC ProServe team is in discovery efforts to understand what our customers are seeking to learn with regard to GDPR. If you have anything you would like to share please reach out to the ProServe contacts below.
- Current activities underway include:
 - Offering Development: Sales & Delivery Assets targeted for February (legal dependencies)
 - Partner Development: Working with some of our Partners to build/create go to market information.
 - Customer Engagement: Webinars are planned to support Venture Capital Business; if you are interested please reach out.
 - Security Summit/Lofts: Will be present to at several events to support customers onsite

AWS & The GDPR




The European Union's General Data Protection Regulation (GDPR) protects European Union data subjects' fundamental right to privacy and the protection of personal data. It introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance.

AWS services will comply with the GDPR when it becomes enforceable on May 25, 2018.

In addition to our own compliance, AWS is committed to offering services and resources to our customers to help them comply with GDPR requirements that may apply to their activities. New Features are launched regularly, AWS has **500+ features and services** focused on security and compliance.


DOWNLOAD WHITEPAPER

[Navigating GDPR Compliance on AWS](#)



DOWNLOAD WHITEPAPER

[Addressing Data Residency with AWS](#)





Thank You

