



# Enabling Compliance with the General Data Protection Regulation (GDPR) on AWS

Christian Hesse

Amazon Web Services



# What we will cover

1

What is the GDPR?

- *All about protecting personal data*

2

What comes with the GDPR?

- *Applies beyond the EU*

3

Who does the GDPR apply to?

- *An overview*

4

Shared responsibilities under the GDPR?

- *AWS's role under GDPR*

5

How AWS can help customers?

- *Technical and organizational measures*

6

Code of Conducts

- *The CISPE Code of Conduct*

7

How Partners and AWS ProServe could help customers



**“AWS welcomes the arrival of the GDPR.** The new, robust requirements raise the bar for data protection, security, and compliance, and will push the industry to follow the most stringent controls, helping to make everyone more secure”

- **Stephen Schmidt**, Chief Information Security Officer, AWS, April 25, 2017

<https://aws.amazon.com/blogs/security/aws-and-the-general-data-protection-regulation/>



“Today, I’m very pleased to announce that **AWS services comply with the General Data Protection Regulation (GDPR)**. This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, **customers can deploy AWS services as a key part of their GDPR compliance plans.**”

- **Chad Woolf**, Vice President, Security Assurance, March 26, 2018

<https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/>



# 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 since **25 May 2018**, and it replaced the EU Data Protection Directive (Directive 95/46/EC)

# 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"

# GDPR applies beyond the EU



Is the customer using AWS to process personal data? If YES

Then GDPR applies if:

The customer is established in the EU  
OR

The customer is established outside the EU,  
but is either offering goods or services to individuals in the EU, OR  
monitoring the behavior of individuals in the EU







# What comes with the GDPR?



# 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 of the personal data that **controllers** have regarding him or herself. 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.





**Who does the GDPR apply to?**

# GDPR Core Concepts



An **identified** or **identifiable**  
person residing in the EU



# GDPR Core Concepts



Determines the **purpose and means of the processing** of **personal data**.



An **identified** or **identifiable** person residing in the EU



Customers control how they configure their environment and secure content.





# GDPR Core Concepts



Determines the **purpose and means of the processing** of **personal data**.

Processes **personal data** on behalf of the controller.



An **identified** or **identifiable** person residing in the EU



Customers control how they configure their environment and secure content.



Carries out operations on personal data, such as collection, use, **storage**, alteration, retrieval, disclosure, making available.

# Bringing it all together



**Controllers *and* Processors have obligations under GDPR**



# Shared responsibility under the GDPR?

# GDPR in practice: implementing TOMs



Under GDPR, **controllers** and **processors** are required to implement appropriate technical and organisational 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

# AWS 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

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

## AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global  
Infrastructure

Availability Zones

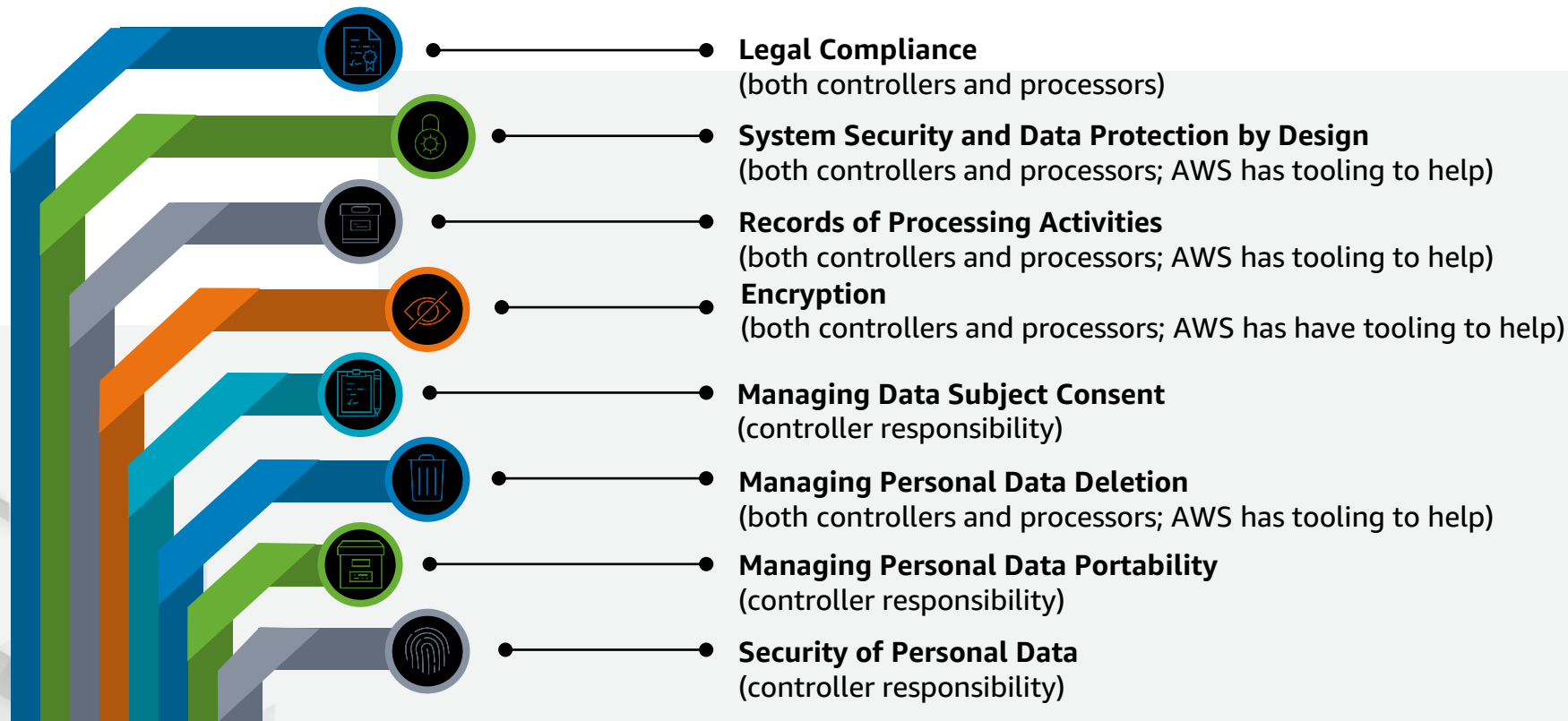
Regions

Edge Locations

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



# GDPR is also a “shared responsibility”





# How AWS can help customers achieve GDPR compliance?

# Navigating GDPR Compliance with AWS Services

*'Data protection by design and default'*



AWS  
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

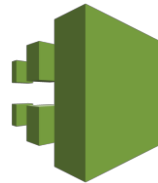


Server-side  
Encryption

*'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**

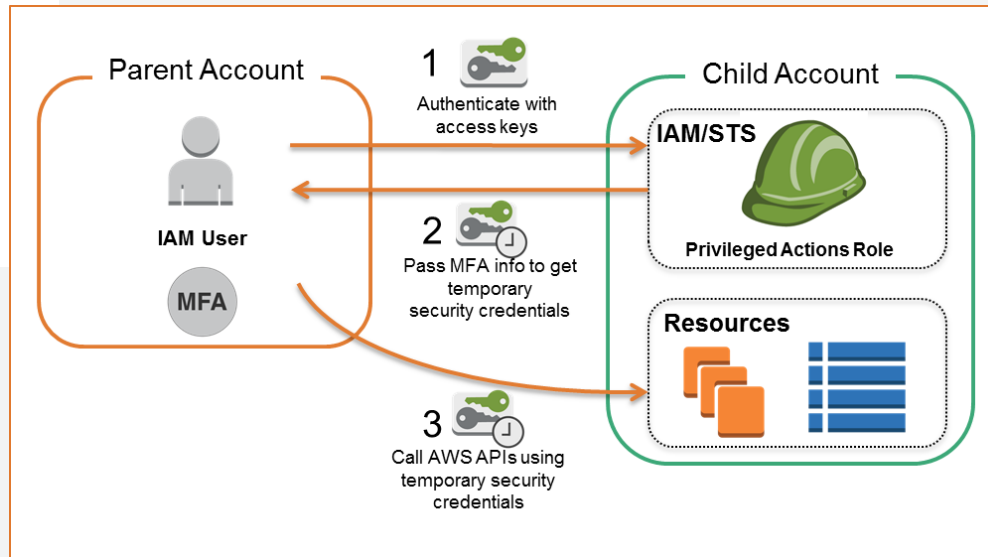
The **controller** “shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.”

**Multi-factor authentication**  
**API-Request Authentication**  
**Temporary Access Tokens**

# AWS & The GDPR



## Access Control



# 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.”

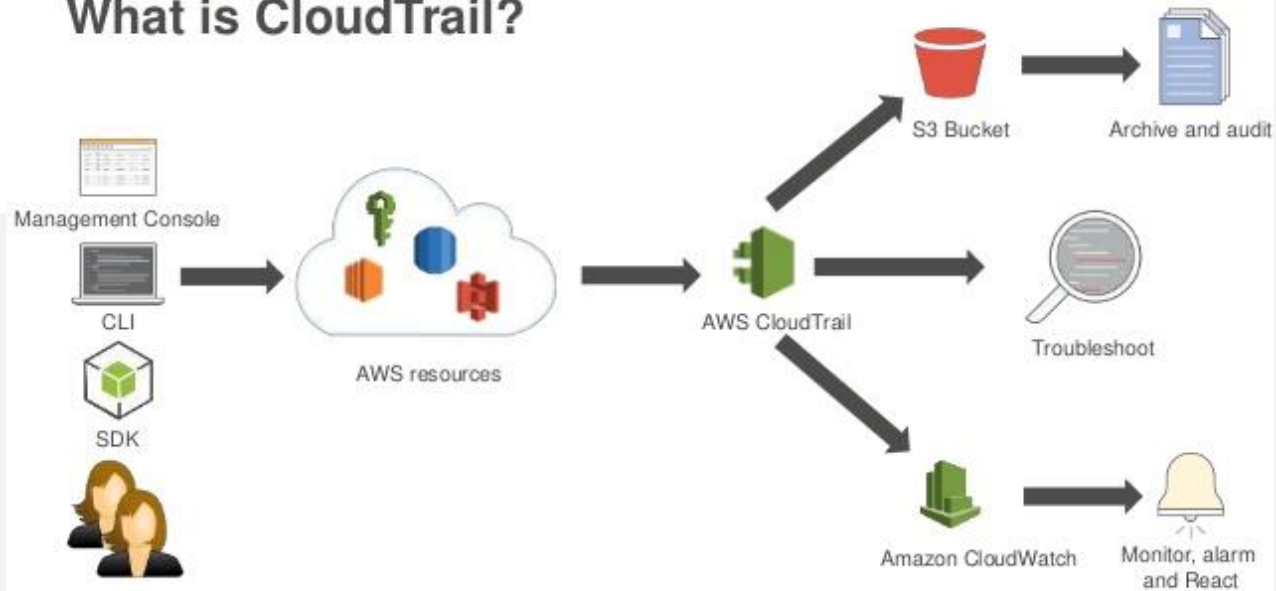
**CloudTrail**  
**Amazon Inspector**  
**Macie**  
**AWS Config**

# AWS & The GDPR



## Monitoring and Logging

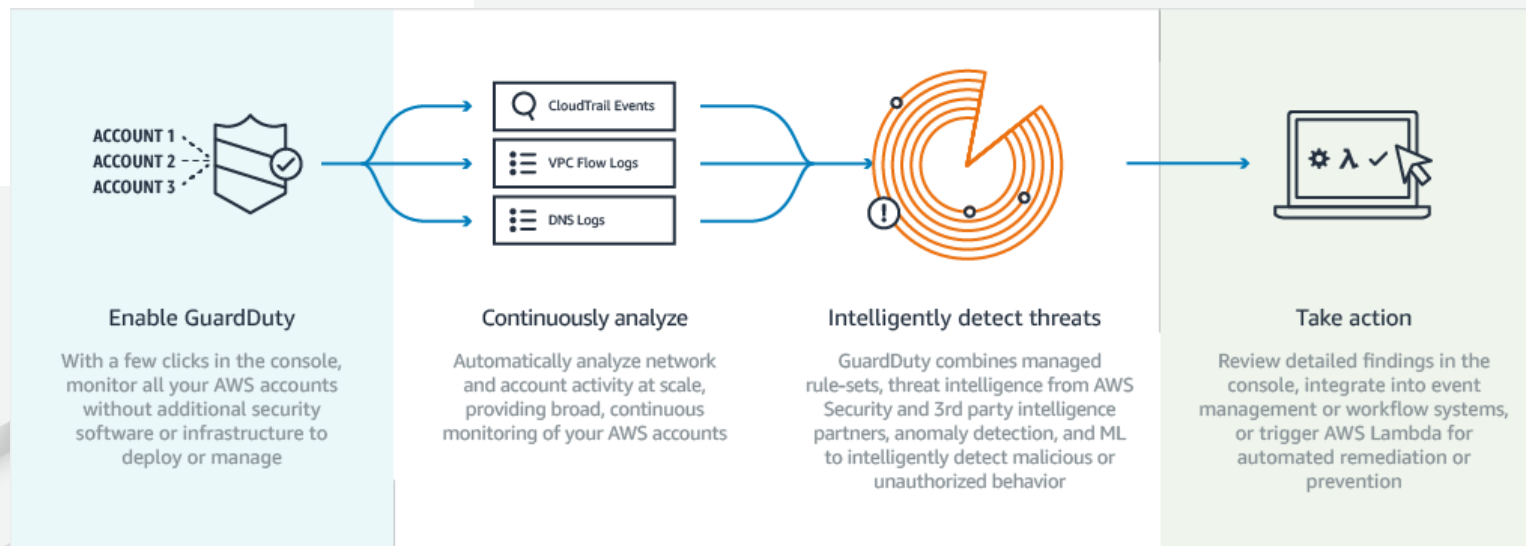
### What is CloudTrail?



# AWS & The GDPR



## Amazon GuardDuty



# GDPR Compliance Tools



**Data Access  
Control**

**Monitoring of  
Access Activities**

**Data  
Encryption**

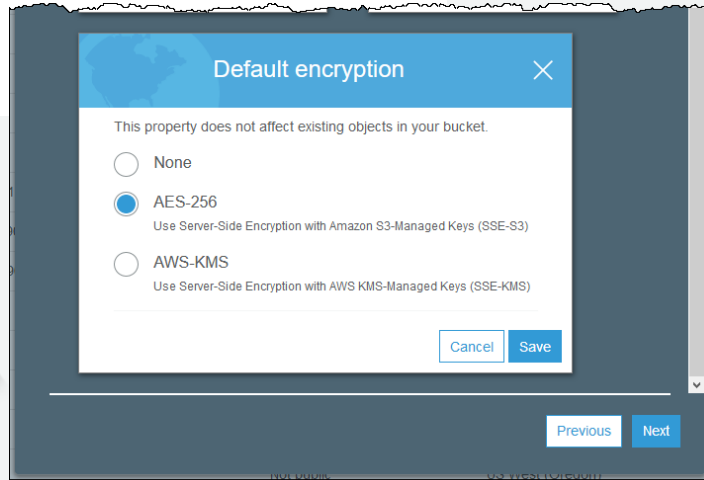
**Strong Compliance  
Framework**

Organisations must “implement appropriate technical and organisational 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/Amazon Glacier/RDS)  
Centralised (by Region) with Key Management (AWS KMS)  
IPsec tunnels into AWS with the VPN-Gateways  
Dedicated HSM modules in the cloud with CloudHSM**

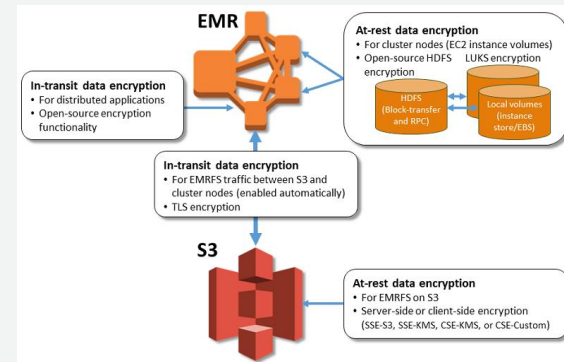
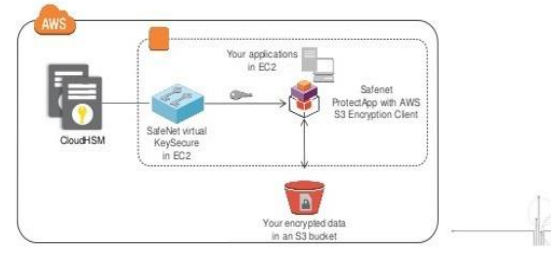
# AWS & The GDPR

## Encryption



### S3 Encryption

Encryption of S3 objects using master keys in CloudHSM



# GDPR Compliance Tools



**Data Access  
Control**

**Monitoring of  
Access Activities**

**Data  
Encryption**

**Strong Compliance  
Framework**

Appropriate technical and organisational 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  
Conduct

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



# Code of Conducts?

# GDPR – Code 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



# How Partners and AWS ProServ could help customers?





# AWS Marketplace: One-stop shop for **familiar** tools



## Advanced Threat Analytics



## Application Security



## Identity and Access Mgmt



## Server & Endpoint Protection



## Network Security



## Encryption & Key Mgmt



## Vulnerability & Pen Testing



# AWS Partner Network (APN) & the 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.



**FORTINET®**



evident.io

# AWS Professional Services



## Privacy by Design Workshop

- **Objective**

- Educate and enable customers on how to architect their AWS environment to support data protection and privacy

- **Audience**

- Legal/Privacy Teams
- Regulatory & Compliance Staff
- Application, Systems & Database Architects

- **Duration**

- One Day Workshop

# Key Activities



- **Earn Trust**

- Introduction/Review of AWS Compliance Programs
- Review AWS Compliance Programs supporting Data Privacy

- **Learn & Educate**

- Provide concept of Data Protection as a Shared Responsibility
- About the customers current architecture
- Learn about how the customer has interpreted the regulation and the controls
- AWS services and features to support technical implementations
- Data Processing Addendum

- **Identify**

- Identify APN Partners and Solutions which can be leveraged in development and operations to achieve data protection efforts





# Data Protection Terms



# Data Protection Terms



- **Customers do not need additional or separate terms relating to GDPR.** The data processing terms are included in our online Service Terms.
- **Customers with existing DPAs could sign GDPR ready DPA**

**Available to ALL  
customers online!**

## AWS Service Terms

Last updated: February 20, 2018

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the **"Agreement"**), the terms and conditions of these Service Terms apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

### 1. Universal Service Terms (Applicable to All Services)

**1.1.** You may only use the Services to store, retrieve, query, serve, and execute Your Content that is owned, licensed or lawfully obtained by you. As used in these Service Terms, (a) "Your Content" includes any "Company Content" and any "Customer Content" and (b) "AWS Content" includes "Amazon Properties". As part of the Services, you may be allowed to use certain software (including related documentation) provided by us or third party licensors. This software is neither sold nor distributed to you and you may use it solely as part of the Services. You may not transfer it outside the Services without specific authorization to do so.

**1.2.** You must comply with the current technical documentation applicable to the Services (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site. In addition, if you create technology that works with a Service, you must comply with the current technical documentation applicable to that Service (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site.

**<https://aws.amazon.com/service-terms/>**



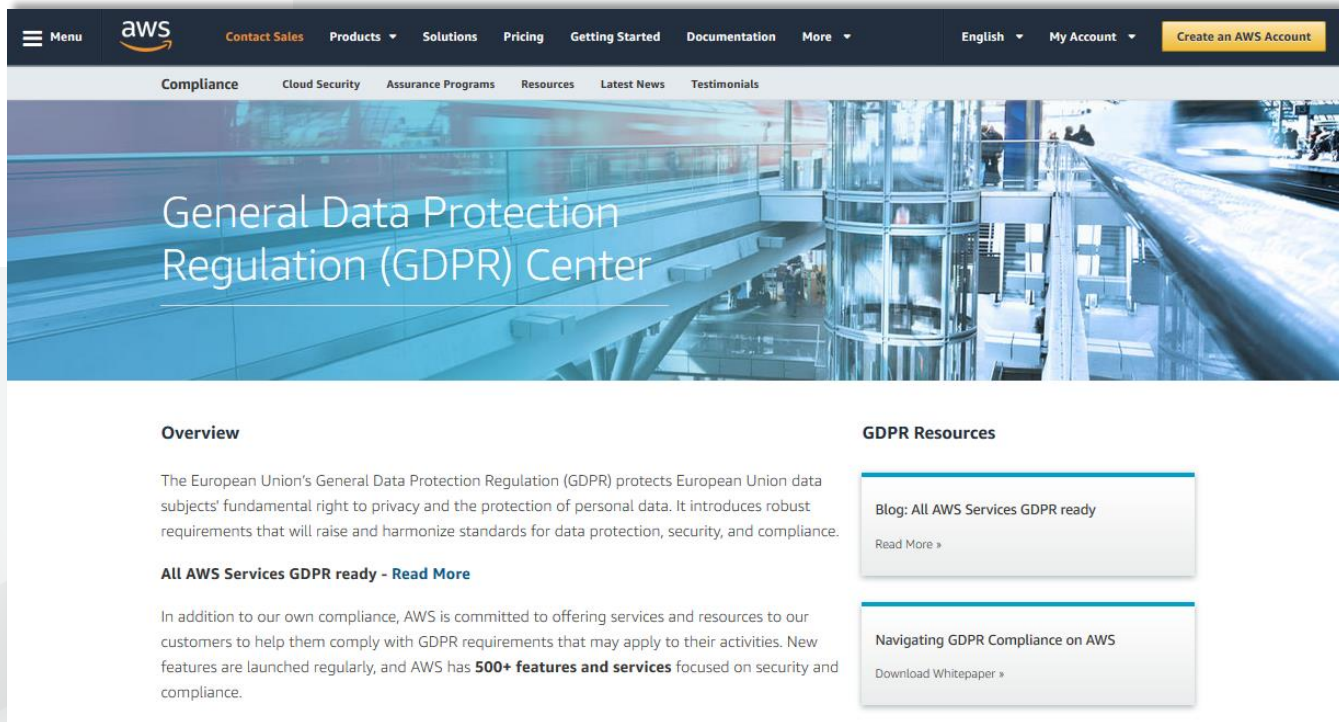
# Resources



# GDPR Center



<https://aws.amazon.com/compliance/gdpr-center/>

A screenshot of the AWS GDPR Center website. The page has a dark blue header with the AWS logo, navigation links like "Menu", "Contact Sales", "Products", "Solutions", "Pricing", "Getting Started", "Documentation", and "More", and user links like "English", "My Account", and a "Create an AWS Account" button. Below the header is a sub-navigation bar with "Compliance", "Cloud Security", "Assurance Programs", "Resources", "Latest News", and "Testimonials". The main content area features a large blue-tinted image of a modern building interior with the title "General Data Protection Regulation (GDPR) Center". Below this, there are two columns: "Overview" and "GDPR Resources". The "Overview" section contains a paragraph about GDPR and a link "All AWS Services GDPR ready - Read More". The "GDPR Resources" section contains two boxes: "Blog: All AWS Services GDPR ready" with a "Read More" link, and "Navigating GDPR Compliance on AWS" with a "Download Whitepaper" link.

**Overview**

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.

**All AWS Services GDPR ready - [Read More](#)**

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, and AWS has **500+ features and services** focused on security and compliance.

**GDPR Resources**

**Blog: All AWS Services GDPR ready**  
[Read More »](#)

**Navigating GDPR Compliance on AWS**  
[Download Whitepaper »](#)

