



AWS Whitepaper

Navigating GDPR Compliance on AWS



Navigating GDPR Compliance on AWS: AWS Whitepaper

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

- Navigating GDPR Compliance on AWS 1**
- Abstract 2**
- Overview of this Whitepaper about Navigating GDPR Compliance on AWS 3**
- GDPR Overview 4**
 - GDPR Requirements for Organizations Operating in the EU 4
 - AWS and the GDPR 4
 - AWS Data Processing Addendum (DPA) 5
 - The Role of AWS Under the GDPR 6
 - AWS as a Processor 7
 - AWS as a Controller 7
 - AWS metadata processing 7
 - Shared Security Responsibility Model 7
 - AWS and Law Enforcement Information Requests 8**
 - Data Protection Impact Assessments (DPIA) Support 8**
 - Data Transfer Impact Assessment (DTIA) Support 9**
 - Incident Response and Breach Notification 10
 - Getting Started with GDPR Compliance on AWS 10
 - Example Step-by-Step GDPR Compliance Process 11
 - Future Considerations 12
- Strong Compliance Framework and Security Standards 14**
 - AWS Compliance Programs 14
 - ISO/IEC 27701 15
 - Cloud Computing Compliance Criteria Catalog (C5) 15
 - The CISPE Data Protection Code of Conduct 16
- Data Access Controls 18**
 - AWS Identity and Access Management (IAM) 18
 - Managing access in the AWS Cloud 18
 - Organizing access across accounts 18
 - Detecting unintended access with IAM Access Analyzer 19
 - Monitoring root account usage and detecting threats 19
 - Refining permissions with access history 19
 - Temporary Access Tokens Through AWS STS 19
 - Multi-Factor-Authentication 20
 - Access to AWS Resources 21

- Defining Boundaries for Regional Services Access 22
 - AWS Control Tower 23
- Control Access to Web Applications and Mobile Apps 24
- Monitoring and Logging 25**
 - Manage and Configure Assets with AWS Config 25
 - Compliance Auditing and Security Analytics 26
 - Collecting and Processing Logs 28
 - Discovering and Protecting Data at Scale with Amazon Macie 29
 - Centralized Compliance and Security Management 31
 - Using AWS Services to Strengthen Compliance and Governance 32
 - AWS Control Tower 23
 - AWS Security Hub 33
 - Amazon GuardDuty 34
 - Amazon Inspector 34
 - Amazon EventBridge 34
 - AWS Organizations 35
 - AWS Systems Manager 35
 - AWS Security Lake 35
 - AWS Audit Manager 36
 - AWS Trusted Advisor 36
 - Amazon Macie 37
- Protecting your Data on AWS 38**
 - Encrypt Data at Rest 38
 - Encrypt Data in Transit 39
 - Encryption Tools 40
 - AWS Key Management Service 41
 - AWS CloudHSM 43
 - AWS Cryptographic Services and Tools 44
 - Pseudonymization 46
 - Data Protection by Design and by Default 46
 - AWS Nitro Enclaves 47
- How AWS Can Help 49**
- Contributors 52**
- Document history 53**
- Notices 54**
- Annex: AWS Customer EU Data Transfer Assessment Guide 55**

Data Transfer Assessment Information 56

- In summary 56
- In detail 57
 - STEP 1: KNOW YOUR TRANSFERS 57
 - STEP 2: IDENTIFY THE TRANSFER TOOLS YOU ARE RELYING ON 64
 - STEP 3: ASSESS THE LAWS OR PRACTICES OF THE COUNTRIES THAT MAY IMPINGE ON THE EFFECTIVENESS OF THE TRANSFER TOOL 65
 - STEP 4: ADOPT SUPPLEMENTARY MEASURES IF REQUIRED 67
 - STEP 5: PROCEDURAL STEPS IF YOU HAVE IDENTIFIED EFFECTIVE SUPPLEMENTARY MEASURES 70
 - STEP 6: RE-EVALUATE AT APPROPRIATE INTERVALS 70

Navigating GDPR Compliance on AWS

Publication date: February 19, 2026 ([Document history](#))

Abstract

This document provides information about services and resources that Amazon Web Services (AWS) offers customers to help them align with the requirements of the General Data Protection Regulation (GDPR) that might apply to their data processing activities. These include adherence to data protection standards, the AWS Cloud Computing Compliance Criteria Catalog (C5) attestation, adherence to the Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct, data access controls, monitoring and logging tools, encryption, and key management. Additionally, this paper provides a dedicated Annex, **AWS Customer EU Data Transfer Assessment Guide**, which outlines practical steps and supplementary measures that customers can follow to assess and secure international data transfers in line with recommendations from the European Data Protection Board (EDPB).

Overview of this Whitepaper about Navigating GDPR Compliance on AWS

This document outlines key GDPR requirements, describes AWS' strong compliance framework and security standards as well as data access controls that help customers to meet their obligations to implement technical and organizational measures under the GDPR. It also describes the monitoring and logging services as well as the encryption services offered by AWS. A detailed Annex, titled "AWS Customer EU Data Transfer Assessment Guide," presents practical steps and supplementary measures based on recommendations from the EDPB to help customers manage international data transfers securely.

GDPR Overview

The GDPR is a European data protection law (Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016) that became enforceable on May 25, 2018. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC), and harmonized data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each EU Member State.

The GDPR applies to:

- Organizations in the EU that process personal data, regardless of whether the processing takes place in the EU.
- Organizations outside the EU that process personal data of individuals located in the EU, where the processing relates to offering goods or services to or monitoring the behavior of individuals in the EU.

Personal data means any information relating to an identified or identifiable natural person. This includes names, identification numbers, location data, online identifiers, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.


GDPR Requirements for Organizations Operating in the EU

One of the key aspects of the GDPR is that it creates consistency across EU Member States on how personal data may be processed, used, and exchanged securely. Organizations must demonstrate their compliance with the GDPR on an ongoing basis, e.g. by maintaining appropriate technical and organizational measures.

AWS and the GDPR

AWS customers can use all AWS services to process personal data (as defined in the GDPR) that is uploaded to the AWS services under their AWS accounts (customer data) in compliance with the GDPR. In addition to our own compliance, AWS is committed to offering services and resources to our customers to help them comply with the 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.

AWS compliance, data protection, and security experts work with customers around the world to answer their questions and help them prepare to run workloads in the cloud under the GDPR.

 **Note**

Note: All AWS services can be used in compliance with the GDPR.

AWS Data Processing Addendum (DPA)

AWS offers a GDPR-compliant [AWS Data Processing Addendum](#) (AWS DPA), which enables AWS customers to comply with GDPR contractual obligations. The AWS DPA is incorporated into the [AWS Service Terms](#) and applies automatically to all customers globally whenever customers use AWS services to process customer data, regardless of which data protection laws apply to that processing.

Customers can transfer their content from Europe to the US and other countries using AWS, in compliance with EU data protection laws, including the GDPR. For example, where AWS customers choose to transfer customer data outside the EU to a country not recognized by the European Commission as providing an adequate level of protection for personal data subject to the GDPR, AWS uses the Standard Contractual Clauses (SCCs) as a data transfer tool to validate such transfers (unless AWS has adopted an alternative recognized compliance standard for lawful data transfers). The SCCs are part of the AWS Service Terms, are incorporated by reference into the AWS DPA, and apply automatically in case of such a data transfer. As the regulatory and legislative landscape evolves, AWS remains committed to ensuring that customers can continue to benefit from AWS globally.

In February 2021, AWS adopted strengthened contractual commitments for protecting customer data. These commitments apply to all customer data processed by AWS, regardless of whether it is transferred outside the European Economic Area (EEA). These commitments are automatically available to all customers using AWS to process their customer data, without any additional action required, through a [Supplementary Addendum](#) to the AWS DPA, which is incorporated in the AWS Service Terms.

The key commitments outlined in the Supplementary Addendum include:

- Redirecting governmental requests for customer data directly to customers whenever possible.
- Promptly notifying customers if AWS is compelled to disclose customer data (unless prohibited by law), allowing customers time to seek protective measures.

- Actively challenging governmental requests that are overly broad, inappropriate, or conflict with EU or applicable EU Member State laws.
- Disclosing only the minimal amount of customer data necessary when legally compelled to do so.

AWS outlines a structured framework to clarify the division of responsibilities in the context of international data transfers under the GDPR. This framework reflects current European regulatory expectations and highlights the shared responsibility model. Under this model, customers are responsible for assessing and implementing the technical and organizational measures needed to secure their data transfers, while AWS remains responsible for maintaining contractual and infrastructure-level safeguards.

The framework includes a practical six-step process based on guidance from the European Data Protection Board (EDPB), which is the independent EU body composed of representatives from national data protection authorities and the European Data Protection Supervisor. The steps help customers: (1) map data transfers; (2) identify the legal transfer mechanism in use (such as SCCs); (3) assess the laws and practices of destination countries; (4) implement supplementary safeguards where necessary; (5) document procedural steps; and (6) reassess risk periodically.

AWS supports customers in this process by offering a set of technical, organizational, and contractual safeguards, such as encryption, data residency controls, and legal commitments to resist overreaching governmental requests. These safeguards help customers meet regulatory expectations and demonstrate accountability. AWS is responsible for implementing and maintaining contractual measures, while customers are responsible for configuring AWS services to reflect their compliance needs and risk posture.

The Role of AWS Under the GDPR

Under the GDPR, AWS may act as either a processor or a controller, depending on the service and how it is used. A controller is the entity that decides why and how personal data is processed. A processor handles personal data only on the controller's behalf and only for the purposes the controller defines. This distinction matters because it determines whether AWS or the customer is responsible for decisions about how personal data is handled and which party is accountable for meeting specific GDPR obligations.

The AWS DPA applies specifically to customer data uploaded and managed by the customer through AWS services.

AWS as a Processor

When AWS customers use AWS services to process customer data in their content, AWS acts as a processor. Customers typically remain as controller and determine the purposes and means of processing. For example, customers can use the controls available in AWS services, including security configuration controls, to process customer data. The [AWS DPA](#) incorporates AWS's commitments as processor or sub-processor.

AWS as a Controller

When AWS collects customer data and determines the purposes and means of processing (e.g., for account registration, administration or customer support), it acts as a controller. The [AWS Privacy Notice](#) describes how AWS collects, uses and discloses customer data where it acts as controller.

AWS metadata processing

AWS acts as a controller for operational metadata it generates or collects to operate services, manage accounts, bill customers and maintain security (such as account IDs, billing information, and security logs). AWS processes such metadata as described in the [AWS Privacy Notice](#).

For metadata customers generate or configure through AWS services (customer-created metadata), AWS does not act as processor, since AWS retains control over processing locations and determines other related processing aspects for this metadata.

Shared Security Responsibility Model

AWS follows a shared responsibility model for security and compliance. Under this model, AWS is responsible for the "Security OF the Cloud". This includes protecting the infrastructure that runs AWS services, such as data centers, networks, hardware, and the foundational software that supports services like [Amazon Simple Storage Service \(Amazon S3\)](#) and [Amazon DynamoDB](#).

Customers are responsible for "Security IN the Cloud". This means configuring and managing the security of the AWS services they use. Responsibilities include managing user access, encrypting data, setting up monitoring, and implementing technical and organizational measures to meet their own compliance needs, including under the GDPR.

Under the GDPR, this model remains unchanged. AWS acts as a processor or sub-processor for customer data, while customers act as controllers or processors and retain full control over how

personal data is collected, used, and secured within their AWS environment. Understanding this distinction is essential for customers to assess their compliance needs, especially when conducting data protection impact assessments or evaluating international data transfers.

For more information, see the [AWS Shared Responsibility Model](#).

AWS and Law Enforcement Information Requests

In line with its commitments under the [Supplementary Addendum](#) to the [AWS DPA](#), If AWS receives a legally valid and binding request for customer data, AWS reviews the request to confirm its legal sufficiency and appropriateness. Wherever possible, AWS will redirect the requesting authority to contact the customer directly.

If AWS is legally compelled to disclose customer data, it will notify the customer before providing any data, unless legally prohibited from doing so. AWS challenges requests that are overly broad, inappropriate, or conflict with applicable law. AWS will disclose only the minimum amount of data necessary to comply with the request.

These commitments are part of AWS's broader approach to privacy and customer control. AWS publishes regular [Information Request Reports](#) (e.g., [January – June 2025](#)) summarizing the number and type of requests received. The full policy and process for Law Enforcement is available in the AWS [Law Enforcement Guidelines](#).

Customers can rely on these commitments as part of their own compliance assessments, including for international data transfers and risk-based evaluations under the GDPR.

Data Protection Impact Assessments (DPIA) Support

AWS customers, as controllers, are responsible for determining when a Data Protection Impact Assessment (DPIA) is required under Article 35 of the GDPR and for conducting such DPIA. AWS supports customers by providing tools and documentation to help identify and mitigate risks, including:

- [Amazon Macie](#) for sensitive data discovery and classification;
- [AWS CloudTrail](#) for comprehensive logs of activity;
- [AWS Security Hub](#) for centralized security and compliance insights;
- [AWS Artifact](#) for on-demand compliance reports; and
- [AWS Organizations](#) for multi-account management capabilities.

- In line with the shared responsibility model, AWS secures the infrastructure and necessary tooling, while customers are responsible for determining when a DPIA is necessary and conducting the assessment in accordance with GDPR requirements.

Data Transfer Impact Assessment (DTIA) Support

Customers, as controllers, must conduct their own Data Transfer Impact Assessments (DTIAs) for international data transfers. In line with the shared responsibility model, AWS supports customers by providing the necessary tools and resources for such transfers, but does not conduct the assessments.

Customers can use AWS services with confidence that their data remains in the AWS Region they select. Only a small number of AWS services involve the transfer of customer data, for example, to develop and improve those services, where you can opt-out of the transfer, or because the transfer is an essential part of the service (such as a content delivery service). AWS's systems are designed to prevent remote access by AWS personnel to customer data unless specifically requested by the customer or required by law. More information is available on the "[Privacy Features of AWS Services](#)" webpage.

[AWS Control Tower](#) and [regional](#) services enable customers to implement strict data residency controls. Supplementary measures include strong encryption controls through [AWS Key Management Service \(AWS KMS\)](#) and [AWS CloudHSM](#), robust access controls through [AWS Identity and Access Management \(AWS IAM\)](#) and comprehensive logging through [AWS CloudTrail](#).

To facilitate international data transfers, AWS also provides the appropriate data transfer mechanisms, such as the SCCs, which are part of the AWS Service Terms and incorporated by reference into the AWS DPA to validate data transfers from the EEA to countries not recognized by the European Commission as providing an adequate level of protection for personal data subject to GDPR. AWS has also certified to the EU-US Data Privacy Framework (DPF) and adheres to the DPF Principles, providing another relevant transfer mechanism. You can view the AWS DPF certification [here](#). Please note that to locate the certification, search for "Amazon" in the search bar as AWS is one of the covered entities under the Amazon.com, Inc. certification. For more detailed guidance on international data transfers, please see the Annex "AWS Customer EU Data Transfer Assessment Guide" below.

Incident Response and Breach Notification

AWS provides a comprehensive set of tools and services to help customers detect, respond to, and report potential data breaches within the GDPR's 72-hour notification requirement. Customers should integrate these tools and services into their broader incident response plans, which should include procedures for assessing breach severity, determining notification requirements, and coordinating with Data Protection Authorities. Customers should also regularly test their incident response procedures through simulations to ensure they can meet the GDPR's strict notification requirements.

Getting Started with GDPR Compliance on AWS

AWS makes available services, features, and documentation that customers can use to configure their environments in alignment with GDPR requirements. Customers remain responsible for evaluating their own use of AWS services and defining their individual compliance approach.

To get started, customers should consider the following structured process:

- **Understand your notification obligations:** Before designing your cloud architecture, ensure you are ready to meet key GDPR obligations, such as the 72-hour breach notification requirement under Article 33 of the GDPR. AWS provides tools like [Amazon GuardDuty](#), [AWS CloudTrail](#), and [AWS Security Hub](#) to support incident detection and response, but customers must establish procedures for severity assessment, notification decisions, and regulator coordination.
- **Conduct a data processing assessment:** Identify what personal data is being processed, for what purposes, and where it flows. This includes reviewing data types, processing activities, and any cross-border transfers. Map these findings to the AWS services and accounts you use or plan to use.
- **Design your account and service architecture:** Use [AWS Organizations](#) and [AWS Control Tower](#) to implement a structured multi-account setup. This can help isolate workloads, manage permissions, and enforce guardrails from the beginning.
- **Define your compliance roadmap:** Plan and implement the required technical and organizational measures. This typically includes:
 - Technical: encryption, access management, logging, and monitoring
 - Organizational: privacy policies, consent handling, DPIA processes, and staff training

- **Assign clear roles and responsibilities:** Ensure all key stakeholders are identified early, including Data Protection Officers (DPOs), legal counsel, and technical leads. Each must understand their part in maintaining compliance.
- **Establish and maintain documentation:** Tools like [AWS CloudTrail](#), [AWS Config](#), [AWS Security Hub](#) and [AWS Audit Manager](#) can help create and maintain an evidence-based assessment framework aligned with GDPR requirements.
- **Plan for continuous compliance:** Implement processes for ongoing monitoring, regular reviews, and incident response. AWS provides various templates, checklists, and technical documentation through [AWS Prescriptive Guidance](#) and [AWS Solutions Library](#) to help customers implement GDPR-compliant architectures.

AWS provides infrastructure and service-level controls, and customers are responsible for defining their data protection strategy, configuring services, and managing compliance over time.

Example Step-by-Step GDPR Compliance Process

This section provides an example step-by-step approach, based on common practices, for customers to get started with their GDPR compliance on AWS:

- *Data Inventory, Purpose for Processing, and Mapping:* Identify all personal data processed and for which purposes; map the data flows, including cross-border transfers.
- *GDPR Readiness Assessment:* Evaluate current compliance status against GDPR requirements; identify gaps in policies, procedures, and technical measures.
- *Establish a Governance Structure:* Appoint key roles (e.g., Data Protection Officer if required); Define responsibilities and reporting lines; set up a cross-functional GDPR compliance team.
- *Update Policies and Procedures:* Review and update privacy policies, consent mechanisms; develop procedures for handling data subject rights; and create data retention and deletion policies.
- *Implement Technical Measures:* Enable encryption for data at rest and in transit; set up access controls and authentication; implement logging and monitoring including a mechanism for sensitive data discovery; use [AWS Well-Architected Framework](#) to guide secure and compliant design.
- *Conduct Data Protection Impact Assessments (DPIAs):* Identify high-risk processing activities and perform DPIAs for these activities.

- *Implement Data Subject Rights Processes:* Set up mechanisms to handle access, deletion, and portability requests; implement data rectification processes.
- *Establish Breach Notification Procedures:* Develop an incident response plan; set up detection and notification systems; conduct breach notification drills.
- *Training and Awareness:* Conduct GDPR training for staff; create role-specific guidance for teams; use AWS training resources to support cloud-specific compliance knowledge.
- *Documentation and Record-Keeping:* Maintain records of processing activities, document compliance measures and decisions; use [AWS CloudTrail](#) and [AWS Config](#) for maintaining audit trails.
- *Continuous Monitoring and Improvement:* Regularly review and update compliance measures; stay informed about AWS service updates and new compliance features; conduct periodic audits and assessments.

Remember, this is a general approach and should be tailored to each organization's specific circumstances and use of AWS services. It is advisable to consult with legal and privacy professionals familiar with the GDPR and AWS to ensure comprehensive compliance.

Future Considerations

As the regulatory landscape and technology continue to evolve, organizations must stay vigilant and adaptable in their GDPR compliance efforts on AWS. AWS closely monitors new developments and updates its services and assurances accordingly. Customers should regularly review AWS's compliance resources and service updates to leverage new features that can enhance their GDPR compliance posture.

Managing Cross-Border Data Transfers

Transferring personal data outside the EU requires careful consideration of evolving regulatory expectations. While AWS offers SCCs, adherence to the DPF, and other mechanisms that enable compliant transfers, customers remain responsible for evaluating the specific context of their transfers and for implementing appropriate safeguards under the GDPR.

Customers should monitor changes such as new adequacy decisions, evolving case law, or updates to guidance from supervisory authorities. These developments may affect risk assessments or the need for supplementary measures. As AWS expands its global infrastructure, customers also have more options to store and process data in specific regions. This flexibility supports data residency, sovereignty, and regulatory alignment.

Customers can take advantage of AWS's multi-region, multi-account capabilities to structure environments that align with different legal requirements, including national restrictions on data location, access, or processing. AWS provides tools that support data residency controls, granular access management, detailed logging, and encryption key management across regions. In addition, AWS regularly updates its compliance programs, guidance, and service-level features to reflect new legal standards and regulatory frameworks.

By using these AWS capabilities as part of a structured compliance strategy, customers can adapt more easily to regulatory change, reduce the need for costly architectural rework, and stay aligned with evolving data protection expectations across jurisdictions.

Strong Compliance Framework and Security Standards

The GDPR requires both controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These may include “...the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services,” (Article 32(1)(b) of the GDPR) as well as reliable data restoration, testing, and overall risk management processes.

To support customers in meeting these obligations, AWS maintains a broad compliance framework grounded in international and regional standards. The following sections describe key components of this framework:

- **AWS Compliance Programs**, which include third-party certifications and independent audit reports available through [AWS Artifact](#).
- **ISO/IEC 27701 certification**, which extends AWS's existing security certifications to cover privacy-specific requirements aligned with the GDPR.
- **Cloud Computing Compliance Criteria Catalogue (C5)**, a German federal standard that provides structured assurance for operational and cybersecurity practices in cloud environments.
- **The CISPE Code of Conduct**, a GDPR-approved pan-European compliance framework specifically for cloud infrastructure providers, under which over 100 AWS services have been independently certified.

Together, these programs and commitments provide customers with validated evidence of the technical and organizational measures AWS has implemented and form a reliable foundation to support their own GDPR compliance efforts. Each of these elements is detailed in the sections below.

AWS Compliance Programs

AWS continually maintains a high bar for security and compliance across all of our global operations. Security is our top priority. AWS regularly undergoes independent third-party attestation audits to provide assurance that control activities are operating as intended. More specifically, AWS is audited against a variety of global and regional security frameworks dependent on region and industry. Currently, AWS offers over 300 security, compliance, and governance services and features. AWS supports 143 security standards and compliance certifications.

The results of these audits are documented by the assessing body and made available for all customers through [AWS Artifact](#). [AWS Artifact](#) is a no-cost, self-service portal for on-demand access to AWS compliance reports. When new reports are released, they are made available in [AWS Artifact](#), allowing customers to continuously monitor the security and compliance of AWS with immediate access to new reports.

Customers can take advantage of internationally recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27017 for cloud security, ISO 27018 for cloud privacy, ISO 27701 for privacy information management, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1 and others. AWS also helps customers meet local and regional data protection standards such as BSI's Cloud Computing Compliance Criteria Catalogue (C5), a German government-backed attestation, and the EU-wide GDPR CISPE Data Protection Code of Conduct (CISPE Code).

ISO/IEC 27701

The AWS ISO/IEC 27701:2019 certification demonstrates that AWS has implemented privacy-specific controls as part of a comprehensive privacy information management system. It validates that AWS has appropriate technical and organizational measures in place to protect personal data, including safeguards for cross-border transfers, data subject rights management, and privacy by design.

Customers can access the AWS ISO 27701 certification through [AWS Artifact](#) and use it as evidence when conducting their own compliance assessments.

ISO/IEC 27701:2019 is an international standard for privacy information management. This certification extends ISO/IEC 27001 to include specific privacy requirements, making it particularly relevant for GDPR compliance. As a Privacy Information Management System (PIMS) standard, ISO 27701 provides a framework for managing personal data and assists organizations in complying with various privacy regulations, including the GDPR. AWS's certification covers the implementation of privacy-specific controls and demonstrates our commitment to protecting personal data through a comprehensive privacy management system. The certification scope includes AWS's role as both a processor and controller, aligning with our dual role under the GDPR.

Cloud Computing Compliance Criteria Catalog (C5)

Customers can use the C5 attestation to evaluate how legal requirements, such as data privacy regulations, internal policies, or specific risk environments, relate to their use of cloud computing

services on AWS. C5 provides a structured framework for assessing security controls and supports compliance reviews by IT, legal, and risk teams.

C5 is an attestation scheme backed by the German government and introduced by the Federal Office for Information Security (BSI). It was designed to help organizations demonstrate operational security against common cyber threats, based on the German government's security recommendations for cloud providers.

The standard defines technical and organizational security requirements relevant to both cybersecurity and data protection. It also includes disclosures on data location, service provisioning, jurisdiction, certifications, and service scope. C5 aligns with the IT-Grundschutz model and introduces cloud-specific control expectations.

Customers and compliance advisors can use the AWS C5 report as formal assurance of the security measures AWS has in place, especially when migrating or operating regulated workloads in Germany or the EU. The report is available through [AWS Artifact](#), AWS's self-service portal for on-demand compliance reports.

The CISPE Data Protection Code of Conduct

CISPE (Cloud Infrastructure Services Providers in Europe) is a coalition of cloud computing leaders serving millions of European customers. The CISPE Data Protection Code of Conduct (CISPE Code) is the first pan-European data protection code of conduct for cloud infrastructure service providers under Article 40 of the GDPR. It was approved by the EDPB in May 2021 and formally adopted by the French Data Protection Authority (CNIL), acting as the competent supervisory authority, in June 2021.

The CISPE Code confirms that cloud infrastructure providers meet GDPR processor requirements and have been independently verified for compliance. It also goes further by requiring providers to offer services that store and process data exclusively within the EEA.

Cloud infrastructure service providers must also commit that they will not access or use any customer data, except as necessary to provide and maintain the declared services. In particular, the cloud infrastructure service providers must commit to not use customer data for their own purposes, including for data mining, profiling or direct marketing. Ernst and Young CertifyPoint (EYCP) independently certified AWS services listed on the CISPE Public Register complying with the CISPE Code. EYCP was the first "monitoring body" accredited by CNIL to verify cloud infrastructure provider's compliance with the CISPE Code.

More than 100 AWS services certified as compliant with the Cloud Infrastructure Services Providers in Europe (CISPE) Data Protection Code of Conduct. They are registered in [CISPE's public register](#) and can also be found within AWS Services in scope of the [AWS Compliance Program](#). This alignment with the CISPE requirements demonstrates our ongoing commitment to adhere to the heightened expectations for data protection by cloud service providers.

AWS supports more security standards and compliance certifications than any other cloud provider, and is continuously reviewing the needs of our customers as the regulatory environment evolves.

Additional Resources on Compliance Programs

For more detailed information about the AWS compliance programs, reports, and third-party attestations, see [AWS Compliance Programs](#). For service-specific information, see [AWS services in scope by Compliance Program](#).

Data Access Controls

Article 25 of the GDPR states that 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”. The following AWS access control mechanisms can help customers comply with this requirement by allowing only authorized administrators, users, and applications to get access to AWS resources and customer data.

AWS Identity and Access Management (IAM)

Managing access in the AWS Cloud

[AWS Identity and Access Management \(IAM\)](#) is a service that allows customers to control who can access AWS resources and under what conditions. It enables fine-grained permission management aligned with the GDPR principle of data protection by design.

When a new [AWS account](#) is created, a [root user](#) is also created with full administrative privileges. AWS strongly recommends that the root user be used only for essential tasks, such as initial account setup or billing administration. For all other activities, customers should create [IAM users](#) or [roles](#) and assign only the permissions necessary to perform specific tasks. This approach aligns with the [principle of least privilege](#) and is foundational to a secure environment.

IAM supports both long-term credentials (for users) and short-term credentials (for roles). For example, customers can use IAM roles to allow an [Amazon EC2](#) instance to access objects in an [Amazon S3](#) bucket or allow a [AWS Lambda function](#) to write logs to [Amazon CloudWatch Logs](#). The same pattern applies when enabling secure access to services such as [Amazon RDS](#), [Amazon DynamoDB](#), or [Amazon Simple Queue Service \(Amazon SQS\)](#).

Organizing access across accounts

Customers managing multi-account environments can use [AWS Organizations](#) to apply [Service Control Policies \(SCPs\)](#) across accounts. SCPs define broad permissions boundaries and can, for instance, restrict actions available to the root user. AWS provides [examples of SCPs](#) to help customers implement common controls.

Detecting unintended access with IAM Access Analyzer

IAM includes features to help customers continuously monitor how access is granted across their environment. [IAM Access Analyzer](#) evaluates resource policies and identifies unintended external access. It supports multiple resource types, including [Amazon S3 buckets](#), [AWS Key Management Service \(KMS\)](#) keys, [Lambda functions](#), and [SQS queues](#).

When used with S3, IAM Access Analyzer can alert customers if a bucket is publicly accessible or shared across AWS accounts. AWS recommends enabling [Block Public Access settings](#) to prevent unintentional exposure. If access is required for a specific use case, customers should test application behavior and apply precise controls.

Monitoring root account usage and detecting threats

[AWS GuardDuty](#) can detect when root credentials are used in ways that may signal a security concern. The system generates findings such as [Policy:IAMUser/RootCredentialUsage](#) when root access is detected, enabling customers to investigate and take action.

Refining permissions with access history

IAM provides [last accessed information](#), a feature that shows when IAM roles, users, or policies were last used.

Temporary Access Tokens Through AWS STS

Customers can use the [AWS Security Token Service \(AWS STS\)](#) to create and provide trusted users with temporary security credentials that grant access to customers' AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that customers provide for their IAM users, with the following differences:

- Temporary security credentials are for short-term use. Customers can configure the amount of time that they are valid, from 15 minutes up to a maximum of 12 hours. After temporary credentials expire, AWS does not recognize them or allow any kind of access from API requests made with them.
- Temporary security credentials are not stored with the user. Instead, they are generated dynamically and provided to the user when requested. When (or before) temporary security credentials expire, a user can request new credentials, if that user has permissions to do so.

These differences provide the following advantages when customers use temporary credentials:

- Customers do not have to distribute or embed long-term AWS security credentials with an application.
- Temporary credentials are the basis for roles and identity federation. Customers can provide access to their AWS resources to users by defining a temporary AWS identity for them.
- Temporary security credentials have a limited customizable lifespan. Because of this, customers do not have to rotate them or explicitly revoke them when they're no longer needed. After temporary security credentials expire, they cannot be reused. Customers can specify the maximum amount of time the credentials are valid.

Multi-Factor-Authentication

For extra security, customers can add two-factor authentication to their AWS account and to IAM users. With multi-factor authentication (MFA) enabled, when customers sign into the [AWS Management Console](#), they are prompted for their credentials (the first factor), as well as an authentication response from their AWS MFA device (the second factor). Customers can enable MFA for their AWS account and for individual IAM users they have created in their account. Customers can also use MFA to control access to AWS service APIs.

For example, customers can define a policy that allows full access to all AWS API operations in [Amazon EC2](#), but explicitly denies access to specific API operations – such as `StopInstances` and `TerminateInstances` – if the user is not authenticated with MFA.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllActionsForEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ]
    }
  ]
}
```

```
],
  "Resource": "*",
  "Conditions": {
    "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
  }
}
}
```

To add an extra layer of security to Amazon S3 buckets, customers can configure [MFA Delete](#), which requires additional authentication to change the versioning state of a bucket and permanently delete an object version. MFA Delete provides added security in the event that your security credentials are compromised.

To use [MFA Delete](#), customers can use either a hardware or virtual MFA device to generate an authentication code. See the [Multi-Factor Authentication page](#) for a list of supported hardware or virtual MFA devices.

Access to AWS Resources

To implement granular access to your AWS resources, customers can grant different levels of permissions to different people for different resources. For example, customers can allow only some users complete access to [Amazon EC2](#), [Amazon S3](#), [Amazon DynamoDB](#), [Amazon Redshift](#), and other AWS Services.

For other users, you can allow read-only access to only some Amazon S3 buckets; permission to administer only some Amazon EC2 instances, or access to only your billing information.

The following policy is an example of one method you can use to allow all actions on a specific Amazon S3 bucket and explicitly deny access to every AWS service that is not Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ],
```

```
},
{
  "Effect": "Deny",
  "NotAction": "s3:*",
  "NotResource": [
    "arn:aws:s3:::bucket-name",
    "arn:aws:s3:::bucket-name/*"
  ]
}
]
```

You can attach a policy to a user or to a role. For other examples of IAM policies, see [Example IAM Identity-Based Policies](#).

Defining Boundaries for Regional Services Access

As a customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. You can choose to store your customer data in any one or more of our European Regions, including EU Regions in France, Germany, Ireland, Italy, Spain, and Sweden. You can also choose to store your customer data in our Regions in Switzerland and in the United Kingdom. Both Switzerland and the United Kingdom have current adequacy decisions under the GDPR permitting the transfer of personal data. You can also use AWS services with the confidence that customer data stays in the AWS Region you select. AWS prohibits – and our systems are designed to prevent – remote access by AWS personnel to customer data for any purpose, including service maintenance, unless that access is requested by you or unless access is required to prevent fraud and abuse, or to comply with law.

IAM policies provide a simple mechanism to limit access to services in specific Regions. You can add a global condition (`aws:RequestedRegion`) to the IAM policies attached to your IAM Principals to enforce this for all AWS services. For example, the following policy uses the `NotAction` element with the `Deny` effect, which explicitly denies access to all of the actions not listed in the statement if the requested Region is not European. Actions in the [Amazon CloudFront](#), [AWS IAM](#), [Amazon Route 53](#), and [AWS Support](#) services should not be denied because these are popular AWS global services.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Sid": "DenyAllOutsideRequestedRegions",
  "Effect": "Deny",
  "NotAction": [
    "cloudfront:*",
    "iam:*",
    "route53:*",
    "support:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "aws:RequestedRegion": [
        "eu-*"
      ]
    }
  }
}
```

This sample IAM policy can also be implemented as a Service Control Policy (SCP) in [AWS Organizations](#), which defines the permission boundaries applied to specific AWS accounts or Organizational Units (OUs) within an organization. This enables you to control user access to regional services in complex multi-account environments.

Geo-limiting capabilities exist for newly launched Regions. Regions introduced after March 20, 2019 are disabled by default. You must enable these Regions before you can use them. If an AWS Region is disabled by default, you can use the AWS Management Console to enable and disable the Region. Enabling and disabling AWS Regions enables you to control whether users in your AWS account can access resources in that Region. For more information, see ["enable or disable AWS Regions in your account"](#).

AWS Control Tower

Using [AWS Control Tower](#), you can configure region deny control which is an elective control with preventive guidance and apply region restrictions to all registered OUs in the Organization. AWS Control Tower offers a group of controls that are designed to enhance your governance over regional boundaries for access to data:

- *Data residency*: Control over the location of your data.

- *Granular access*: Access restrictions that limit all access to your data, unless the access is requested by you, or by a partner whom you trust.
- *Encryption*: Features and controls that help you encrypt data, whether in transit, at rest, or in memory.
- *Resiliency*: Ability to sustain operations through disruption or disconnection, which is essential in the case of events such as supply chain disruption, network interruption, and natural disaster.

Control Access to Web Applications and Mobile Apps

AWS provides services for managing data access control within customer applications. If you need to add user login and access control features to your web applications and mobile apps, you can use [Amazon Cognito](#). Amazon Cognito user pools provide a secure user directory that scales to hundreds of millions of users. To protect the identity of the users, you can add multi-factor authentication (MFA) to your user pools. You can also use adaptive authentication, which uses a risk-based model to predict when you might need another authentication factor.

With [Amazon Cognito Identity Pools](#) (Federated Identities), you can see who accessed your resources and where the access originated (mobile app or web application). You can use this information to create IAM roles and policies that allow or deny access to a resource based on the type of access origin (mobile app or web application) and Identity Provider.

Monitoring and Logging

[Article 30 of the GDPR](#) states that “each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility”. This article also includes details about which information must be recorded when you monitor the processing of all personal data. Controllers and processors are also required to send breach notifications in a timely manner, so detecting incidents quickly is important. To help enable customers to comply with these obligations, AWS offers the following monitoring and logging services.

Manage and Configure Assets with AWS Config

[AWS Config](#) provides a detailed view of the configuration of many types of AWS resources in your AWS account. This includes how the resources are related to one another, and how they were previously configured, so you can see how the configurations and relationships change over time.

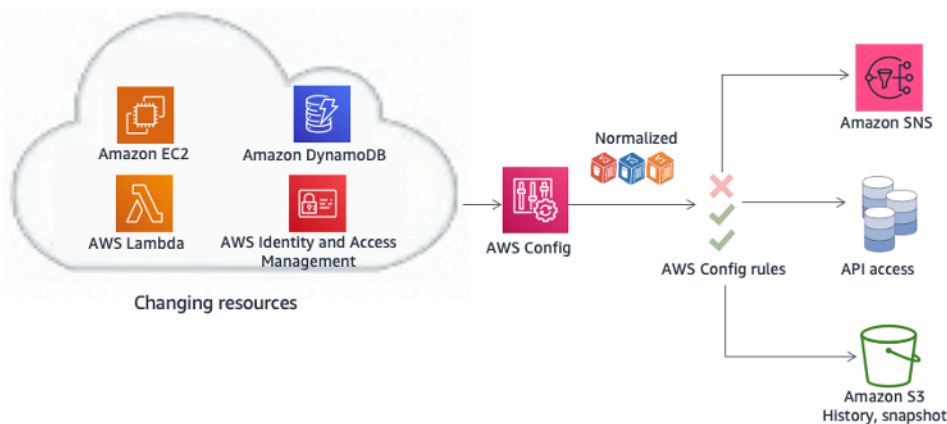


Figure 1 – Monitor configuration changes over time with AWS Config

An AWS resource is an entity that you can work with in AWS, such as an EC2 instance, an [Amazon Elastic Block Store \(amazon EBS\)](#) volume, a security group, or an [Amazon Virtual Private Cloud \(Amazon VPC\)](#). For a complete list of AWS resources supported by AWS Config, see [Supported AWS Resource Types for AWS Config](#).

With AWS Config, you can do the following:

- Evaluate your AWS resource configurations to verify the settings are correct.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS Account.

- Get configurations of one or more resources that exist in your account.
- Get historical configurations of one or more resources.
- Get a notification when a resource is created, modified, or deleted.
- See relationships between resources (for example, find all resources that use a particular security group).

Conformance Packs can be used to simplify the deployment of collections of AWS Config rules and remediation actions and can be used as starting point for creating your own rules.

Compliance Auditing and Security Analytics

With [AWS CloudTrail](#), you can continuously monitor AWS account activity. A history of the AWS API calls for your account is captured, including API calls made through the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators enable and disable CloudTrail logging.

CloudTrail logs can be aggregated from multiple Regions and multiple AWS accounts into a single Amazon S3 bucket. AWS recommends that you write logs – especially AWS CloudTrail logs – to an Amazon S3 bucket with restricted access in an AWS account designated for logging (Log Archive). The permissions on the bucket should prevent deletion of the logs, and they should also be encrypted at rest using Server-Side Encryption with Amazon S3-managed encryption keys (SSE3) or AWS KMS-managed keys (SSE-KMS). CloudTrail log file integrity validation can be used to determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally hard to modify, delete, or forge CloudTrail log files without detection. You can use the AWS command line interface (AWS CLI) to validate the files in the location where CloudTrail delivered them.

CloudTrail logs aggregated in an Amazon S3 bucket can be analyzed for auditing purposes or for troubleshooting activities. Once the logs are centralized, you can integrate with Security Information and Event Management (SIEM) solutions or use AWS services, such as [Amazon Athena](#) or [AWS CloudTrail Insights](#), to analyze them and visualize them using [Amazon Quick Sight Dashboards](#). Once you have CloudTrail logs centralized, you can also use the same Log Archive account to centralize logs from other sources, such as CloudWatch Logs and AWS load balancers.

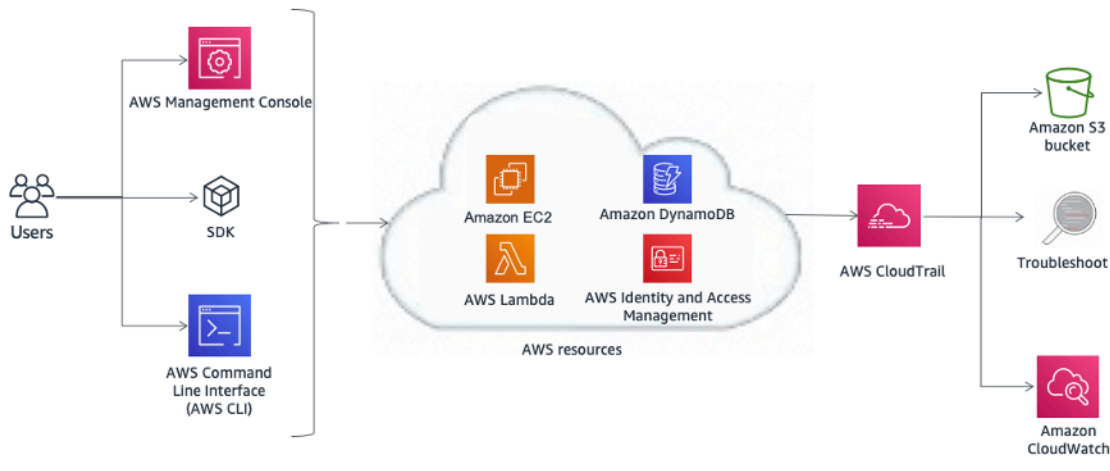


Figure 2 – Example architecture for compliance auditing and security analytics with AWS CloudTrail

AWS CloudTrail logs can also trigger rules configured in [Amazon EventBridge](#), the event-driven service that replaced Amazon CloudWatch Events. You can use these events to notify users or systems that an event has occurred, or for remediation actions. For example, if you want to monitor activities on your Amazon EC2 instances, you can create a CloudWatch Event rule. When a specific activity happens on the Amazon EC2 instance and the event is captured in the logs, the rule triggers an [AWS Lambda](#) function, which sends a notification email about the event to the administrator. (See Figure 3.) The email includes details such as when the event happened, which user performed the action, Amazon EC2 details, and more. The following diagram shows the architecture of the event notification.

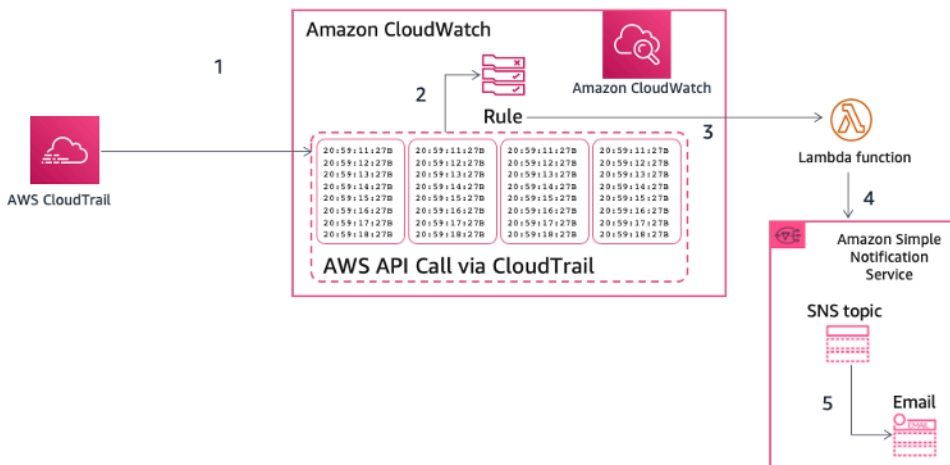


Figure 3 – Example of AWS CloudTrail event notification

Collecting and Processing Logs

[CloudWatch](#) Logs can be used to monitor, store, and access your log files from Amazon EC2 instances, AWS CloudTrail, Route 53, and other sources. See the [AWS Services That Publish Logs to CloudWatch Logs documentation page](#).

Logs information includes, for example:

- Granular logging of access to Amazon S3 objects
- Detailed information about flows in the network through VPC-Flow Logs
- Rule-based configuration verification and actions with AWS Config rules
- Filtering and monitoring of HTTP access to applications with web application firewall (WAF) functions in CloudFront

Custom application metrics and logs can also be published to CloudWatch Logs by installing the CloudWatch Agent on Amazon EC2 instances or on-premises servers.

Logs can be analyzed interactively using CloudWatch Logs Insights, performing queries to help you respond more efficiently and effectively to operational issues.

CloudWatch Logs can be processed in near real-time by configuring subscription filters and delivered to other services such as an [Amazon OpenSearch Service](#) (OpenSearch Service) cluster, an [Amazon Kinesis](#) stream, an [Amazon Data Firehose](#) stream, or [Lambda](#) for custom processing, analysis, or loading to other systems. CloudWatch metric filters can be used to define patterns to look for in log data, transform them into numerical CloudWatch metrics, and set up alarms based on your business requirements. For example, following the AWS recommendation not to use the root user for everyday tasks, it is possible to set up a specific CloudWatch metric filter on a CloudTrail log (delivered to CloudWatch Logs) to create a custom metric and configure an alarm to notify the relevant stakeholders when root user credentials are used to access your AWS account.

Logs such as [Amazon S3 server access logs](#), [Elastic Load Balancing access logs](#), [VPC flow logs](#), and [AWS Global Accelerator flow logs](#) can be delivered directly to an Amazon S3 bucket. For example, when you enable Amazon Simple Storage Service server access logs, you can get detailed information regarding the requests that are made to your Amazon S3 bucket. An access log record contains details about the request, such as the request type, the resources specified in the request, and the time and date the request was processed. For more information about the contents of a log message, see Amazon Simple Storage Service Server Access Log Format in the [Amazon Simple Storage Service User Guide](#). Server access logs are useful for many applications because they give

bucket owners insight into the nature of requests made by clients that are not under their control. By default, Amazon S3 does not collect service access logs, but when you enable logging, Amazon S3 usually delivers access logs to your bucket within a few hours. If you require a faster delivery or need to deliver logs to multiple destinations, consider using CloudTrail logs or a combination of both CloudTrail logs and Amazon S3. Logs can be encrypted at rest by configuring default object encryption in the destination bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or KMS keys (formerly AWS KMS Key) stored in [AWS Key Management Service \(AWS KMS\)](#).

Logs stored in an Amazon S3 bucket can be queried and analyzed using [Amazon Athena](#). Amazon Athena is an interactive query service that enables you to analyze data in S3 using standard SQL. You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena. Athena can process unstructured, semi-structured, and structured data sets and integrates with [Amazon Quick Sight](#) for easy visualization.

Logs are also a useful source of information for automated threat detection. [Amazon GuardDuty](#) is a continuous security monitoring service that analyzes and processes events from several sources, such as VPC Flow Logs, CloudTrail management event logs, CloudTrail Amazon S3 data event logs, and DNS logs. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment. When you enable GuardDuty in a Region, it immediately starts analyzing your CloudTrail event logs. It consumes CloudTrail management and Amazon S3 data events directly from CloudTrail through an independent and duplicative stream of events.

[Amazon Security Lake](#) can be used to automatically centralize security data from AWS environments, SaaS providers, on-premises, and cloud sources into a purpose-built data lake stored in your AWS account. With Security Lake, you can get a more complete understanding of your security data across your entire organization. Security Lake has adopted the Open Cybersecurity Schema Framework (OCSF), an open standard. With OCSF support, the service normalizes and combines security data from AWS and a broad range of enterprise security data sources.

Discovering and Protecting Data at Scale with Amazon Macie

Article 32 of the GDPR states that “[...] the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: [...]

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

[...]

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”

Having an ongoing data classification process is critical for adjusting security data processing to the nature of data. If your organization manages sensitive data, monitor where it resides, protect it properly, and provide evidence that you are enforcing data security and privacy as required to meet regulatory compliance requirements. To help the customer identify and protect their sensitive data at scale, AWS offers [Amazon Macie](#), a fully managed data security and data privacy service that uses pattern matching and machine learning models for detection of Personally Identifiable Information (PII) to discover and protect sensitive data stored in S3 buckets. Amazon Macie scans these buckets and provides a data categorization of them using managed data identifiers that are designed to detect several categories of sensitive data. Amazon Macie can detect PII such as full name, email address, birth date, national identification number, taxpayer identification or reference number, and more. The customer can define custom data identifiers that reflect their organization’s particular scenarios (for example, customer account numbers or internal data classification).

Amazon Macie continually evaluates the objects inside the buckets and automatically provides a summary of findings (Figure 4) for any unencrypted or publicly accessible data discovered that match with the defined data category. This data can include alerts for any unencrypted, publicly accessible objects or buckets shared with AWS accounts outside those you have defined in AWS Organizations. Amazon Macie is integrated with other AWS services, such as [AWS Security Hub](#), to generate actionable security findings and provide an automatic and reactive action to the finding (Figure 5).

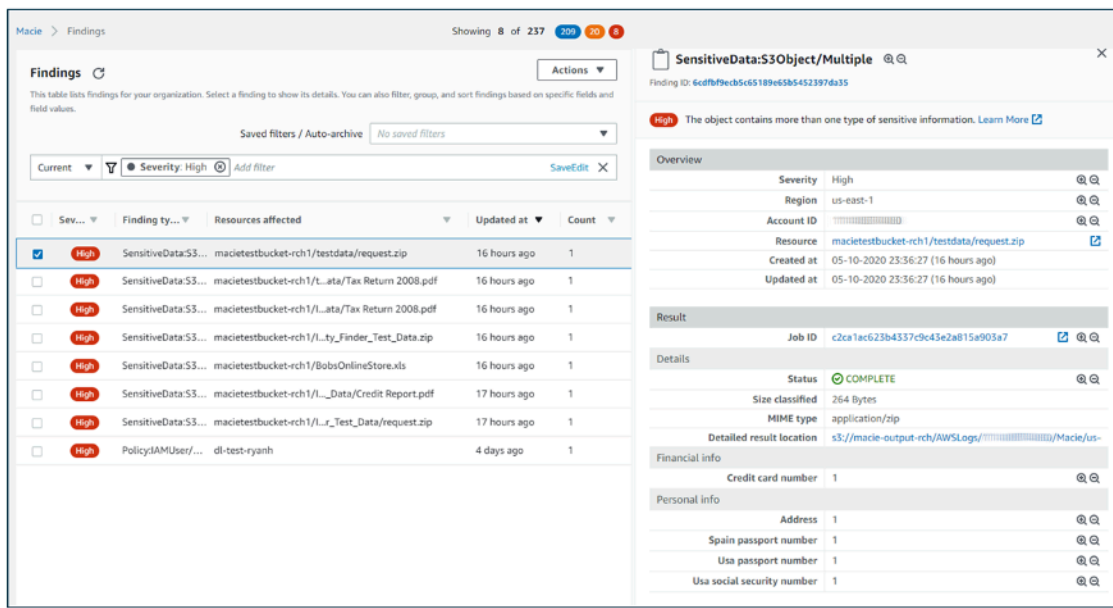


Figure 4 – Data inspections and finding example

In order to prevent sensitive data accidental disclosure, coming from log data in-transit such as credit card numbers or government ID’s logged by your systems, and applications, [Amazon CloudWatch](#) provides data protection account level policy. Account level policies work in combination with log group level policies, allowing you to select patterns of sensitive log data to detect and protect broadly across all log groups in an AWS account. By default, when a user views a log event that includes masked data, the sensitive data is replaced by asterisks according to the policy.

Centralized Compliance and Security Management

Many organizations have challenges related to visibility and centralized management of their environments. As your operational footprint grows, this challenge can be compounded unless you carefully consider your compliance and security architecture. Lack of knowledge, combined with decentralized and uneven management of governance and security processes, can make your environment vulnerable.

AWS provides tools that help you to address some of the most challenging requirements for IT management and governance, and tools for supporting a data protection by design approach.

AWS provides a broad set of integrated services to help customers manage security and compliance across their environments. These services work together to support centralized monitoring, automation, and audit readiness:

- [AWS Security Hub](#) aggregates security findings from services like [Amazon GuardDuty](#), [Amazon Inspector](#), and [Amazon Macie](#), offering a consolidated view of your security posture across AWS accounts and services.
- [AWS Config](#) and [AWS CloudTrail](#) provide the foundational telemetry by tracking configuration changes and logging API activity, feeding critical data into Security Hub and related tools.
- [AWS Audit Manager](#) uses this data to automate evidence collection for compliance assessments aligned with frameworks like the GDPR.
- [AWS Trusted Advisor](#) continuously scans the environment to identify deviations from AWS best practices across cost optimization, security, performance, and fault tolerance.
- [Amazon Detective](#) builds on this by enabling automated security investigations and root cause analysis.
- [AWS Control Tower](#) helps customers establish and govern a secure multi-account AWS environment, including controls for account provisioning, security baselines, and data residency.
- [AWS Organizations](#) allows centralized management of multiple AWS accounts, including policy enforcement and budget controls across an enterprise environment.
- [AWS Key Management Service \(KMS\)](#) and [AWS Identity and Access Management \(IAM\)](#) provide essential tools for managing encryption keys and enforcing fine-grained access control across AWS resources.
- [AWS Security Lake](#) serves as a central repository for security-related data from AWS and third-party sources, enabling advanced analytics and long-term trend analysis through integrations with tools like Amazon Athena and Amazon OpenSearch.

Together, these services support a unified security and compliance architecture where visibility, governance, and automation are built in. This helps organizations meet their regulatory obligations –including under the GDPR – while simplifying operations and reducing risk.

Using AWS Services to Strengthen Compliance and Governance

To meet regulatory obligations such as those under the GDPR, organizations must combine technical, operational, and organizational safeguards. AWS provides a suite of services that help customers implement and manage these safeguards across multi-account cloud environments. The following sections explain how specific AWS services can support key areas of a security and compliance strategy:

- [AWS Control Tower](#) – for setting up and governing secure multi-account environments with built-in guardrails.
- [AWS Security Hub](#) – for centralized visibility into security and compliance findings.
- [Amazon GuardDuty](#) – for intelligent threat detection and analysis of activity logs.
- [Amazon Inspector](#) – for automated vulnerability management and security assessments.
- [Amazon EventBridge](#) (formerly CloudWatch Events) – for triggering automated responses to events and incidents.
- [AWS Organizations](#) – for centralized policy management across multiple accounts.
- [AWS Systems Manager](#) – for operational visibility, automation, and patch compliance.
- [AWS Security Lake](#) – for aggregating and analyzing security data at scale.
- [AWS Audit Manager](#) – for automating evidence collection and managing audit frameworks.
- [AWS Trusted Advisor](#) – for continuous checks and recommendations across security domains.
- [Amazon Macie](#) – for sensitive data discovery and protection across S3 buckets.

AWS Control Tower

[AWS Control Tower](#) provides a method to set up and govern a new, secure, multi-account AWS environment. It automates the setup of a landing zone, which is a multi-account environment that is based on best practices blueprints and enables governance using guardrails that you can choose from a pre-packaged list. Guardrails implement governance rules for security, compliance, and operations.

AWS Control Tower provides identity management using [AWS IAM Identity Center](#) (IAM Identity Center) default directory and enables cross-account audit using IAM Identity Center and IAM. It also centralizes logs coming from CloudTrail and AWS Config logs, which are stored in Amazon S3.

AWS Security Hub

[AWS Security Hub](#) is another service that supports centralization and can improve visibility into an organization. Security Hub centralizes and prioritizes security and compliance findings from across AWS accounts and services, such as [Amazon GuardDuty](#) and [Amazon Inspector](#), and can be integrated with security software from third-party partners to help you analyze security trends and identify the highest priority security issues.

AWS Security Hub Cloud Security Posture Management ([AWS Security Hub CSPM](#)) provides you with a comprehensive view of your security state in AWS and helps you assess your AWS environment against security industry standards and best practices.

Amazon GuardDuty

[Amazon GuardDuty](#) is an intelligent threat detection service that can help customers more accurately and easily monitor and protect their AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes billions of events across your AWS accounts from several sources, including [AWS CloudTrail Management Events](#), [Amazon S3 CloudTrail Events](#), [Amazon Virtual Private Cloud Flow Logs](#), and DNS logs. For example, it detects unusual API calls, suspicious outbound communications to known malicious IP addresses, or possible data theft using DNS queries as the transport mechanism. GuardDuty is able to provide more accurate findings by leveraging machine learning-powered threat intelligence and third-party security partners. GuardDuty Malware Protection helps you detect the potential presence of malware by scanning the [Amazon Elastic Block Store](#) (Amazon EBS) volumes that are attached to the [Amazon Elastic Compute Cloud](#) (Amazon EC2) instances and container workloads. You can include or exclude specific Amazon EC2 instances and container workloads at the time of scanning. You also have an option to retain the snapshots of Amazon EBS volumes attached to the Amazon EC2 instances or container workloads.

Amazon Inspector

[Amazon Inspector](#) is an automated security assessment service that helps improve the security and compliance of applications deployed on Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

Amazon EventBridge

[Amazon EventBridge](#) was formerly called Amazon CloudWatch Events. EventBridge is a serverless service that uses events to connect application components together, making it easier for you to build scalable event-driven applications. Event-driven architecture is a style of building loosely-coupled software systems that work together by emitting and responding to events. Event-driven architecture can help you boost agility and build reliable, scalable applications.

By creating rules in Amazon EventBridge, you can respond automatically to AWS Security Hub CSPM findings. Security Hub CSPM sends findings as events to EventBridge in near-real time. You

can write simple rules to indicate which events you are interested in and what automated actions to take when an event matches a rule. Security Hub CSPM automatically sends all new findings and all updates to existing findings to EventBridge as EventBridge events. You can also create custom actions that allow you to send selected findings and insight results to EventBridge.

AWS Organizations

[AWS Organizations](#) helps you centrally manage and govern complex environments. It enables you to control access, compliance, and security in a multi-account environment. AWS Organizations supports Service Control Policies (SCPs), which define the AWS service actions available to use with specific accounts or Organizational Units (OUs) within an organization.

AWS Systems Manager

[AWS Systems Manager](#) provides you visibility and control of your infrastructure on AWS. You can view operational data from multiple AWS services from a unified console and automate operational tasks across them. You can have information about recent API activities, resource configuration changes, operational alerts, software inventory, and patch compliance status. Using the integration with other AWS services, you can also take action on resources depending on your operational needs, to help make your environment compliant.

For example, by integrating Amazon Inspector with AWS Systems Manager, security assessments are simplified and automated, because you can install Amazon Inspector agent automatically using Amazon Elastic Compute Cloud Systems Manager when an Amazon EC2 instance is launched. You can also perform automatic remediations for Amazon Inspector findings by using Amazon EC2 System Manager and Lambda functions.

AWS Security Lake

[AWS Security Lake](#) provides a comprehensive solution for centralizing security data across your entire organization. It automatically centralizes security data from cloud, on-premises, and custom sources into a purpose-built data lake stored in your account. The service adopts the Open Cybersecurity Schema Framework (OCSF), enabling standardized security data collection and normalization across diverse sources, including AWS services, third-party security solutions, and custom applications. This standardization simplifies security analysis and reporting across your organization. Security Lake automatically creates a copy of your security data in your account's S3 bucket using a column-based Apache Parquet format, optimizing for both storage cost and query performance. The service integrates seamlessly with popular analytics tools like [Amazon](#)

[Athena](#), [Amazon OpenSearch](#), and [Amazon Quick Sight](#), as well as third-party security information and event management (SIEM) solutions. This integration enables security teams to perform more efficient investigations, generate compliance reports, and conduct threat hunting across their entire security data landscape. By providing a unified view of security data, Security Lake helps organizations meet GDPR requirements for continuous monitoring, incident detection, and demonstrable compliance through comprehensive security data management.

AWS Audit Manager

[AWS Audit Manager](#) helps simplify the continuous auditing of AWS usage, making it easier to assess risk and compliance with regulations, industry standards, and company policies. It automatically collects and organizes relevant evidence across AWS accounts and services, mapping it to the controls required for common frameworks such as GDPR, HIPAA, and ISO 27001. The service provides pre-built frameworks that can be customized to align with your organization's specific requirements, while also supporting the creation of custom frameworks for unique compliance obligations. Audit Manager continuously monitors your AWS resource usage and compliance activities, maintaining an audit-ready posture by collecting relevant evidence in the form of configurations, user activity, and compliance results. This evidence is organized into assessments that help demonstrate your compliance posture during audits. The service integrates with other AWS security and compliance tools, including [AWS Security Hub](#), [AWS Config](#), and [AWS CloudTrail](#), to provide a comprehensive view of your compliance status. For organizations managing GDPR compliance, [AWS Audit Manager](#) can help demonstrate ongoing compliance through automated evidence collection and control monitoring, supporting both periodic formal audits and continuous compliance assessments. This automation significantly reduces the manual effort typically required for audit preparation and evidence collection, while providing a centralized view of compliance across your AWS environment.

AWS Trusted Advisor

[AWS Trusted Advisor](#) provides real-time guidance to help customers follow AWS best practices for security, cost optimization, performance, reliability, and service limits. From a security management perspective, Trusted Advisor continuously inspects your AWS environment and provides actionable recommendations across multiple security dimensions. It checks for open access ports, overly permissive permissions, unencrypted data storage, unmanaged encryption keys, and other potential security vulnerabilities. For organizations managing GDPR compliance, Trusted Advisor's security checks are particularly valuable in identifying gaps in data protection measures, such as detecting public S3 buckets that might expose personal data or highlighting IAM configurations that could lead to unauthorized access. The service integrates with [AWS](#)

[Organizations](#) to provide a consolidated view of recommendations across multiple accounts, and works in conjunction with [AWS Security Hub](#) to surface security findings. Through the [AWS Health API](#), customers can programmatically access [Trusted Advisor's](#) recommendations and automate responses to security findings. Enterprise and Business Support customers receive access to the full set of Trusted Advisor checks and can utilize [AWS Config](#) rules based on Trusted Advisor best practices, enabling automated, continuous security assessment and remediation across their AWS infrastructure.

Amazon Macie

[Amazon Macie](#) plays a crucial role in centralized security management by providing automated sensitive data discovery and security assessment across your AWS environment. Using machine learning and pattern matching, Macie automatically discovers and classifies sensitive data such as personally identifiable information (PII), financial data, healthcare information, and credentials stored in Amazon S3 buckets. For GDPR compliance, Macie is particularly valuable as it can identify specific categories of personal data, including European-specific data types such as European tax identification numbers, identity card numbers, and passport information. The service performs continuous analysis of data access patterns and user behavior to detect potential data security risks, such as unencrypted sensitive data or buckets with public access. Macie integrates seamlessly with [AWS Organizations](#) for multi-account management and [AWS Security Hub](#) for centralized findings, enabling organization-wide sensitive data discovery and protection. Through its integration with [AWS EventBridge](#), Macie can trigger automated workflows for remediation actions when it discovers security risks. The service maintains detailed logs of all findings and provides customizable alerts, helping organizations demonstrate their ongoing data protection efforts and respond promptly to potential data privacy incidents. Macie's findings can also be exported to [Amazon Security Lake](#) for long-term analysis and correlation with other security data, providing a comprehensive view of data security posture across the organization.

Protecting your Data on AWS

Article 32 of the GDPR requires that organizations must “[...] implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including [...] the pseudonymization and encryption of personal data [...]”. In addition, organizations must safeguard against the unauthorized disclosure of, or access to personal data.

Encryption reduces the risks associated with the storage of personal data because data is unreadable without the correct key. A thorough encryption strategy can help mitigate the impact of various security events, including some security breaches.

AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for applications and data subject to rigorous contractual or regulatory requirements for managing cryptographic keys, additional protection is sometimes necessary. Previously, the only option to store sensitive data (or the encryption keys protecting the sensitive data) may have been in on-premises datacenters. This might have prevented you from migrating these applications to the cloud, or significantly slowed their performance.

AWS supports encryption at rest and in transit, provides key management options through [AWS KMS](#) and [AWS CloudHSM](#), and enables client-side encryption through libraries like the [AWS Encryption SDK](#). These services help customers comply with data protection regulations and align with industry security standards.

Encrypt Data at Rest

Encrypting data at rest is vital for regulatory compliance and data protection. It helps to ensure that sensitive data saved on disks is not readable by any user or application without a valid key. AWS provides multiple options for encryption at rest and encryption key management. For example, you can use the [AWS Encryption SDK](#) with an [AWS KMS Key](#) created and managed in AWS KMS to encrypt arbitrary data. All AWS services that store customer data offer the ability to encrypt that data.

Encrypted data can be securely stored at rest and can be decrypted only by a party with authorized access to the AWS KMS Key. As a result, you get confidential envelope-encrypted data, policy mechanisms for authorization and authenticated encryption, and audit logging through AWS CloudTrail. Some of the AWS foundation services have built-in encryption at rest features, providing the option to encrypt data before it is written to non-volatile storage. For example, you

can encrypt Amazon EBS volumes and configure Amazon S3 buckets for Server-Side Encryption (SSE) using AES-256 encryption. Amazon S3 also supports client-side encryption, which allows you to encrypt data before sending it to Amazon S3. AWS SDKs support client-side encryption to facilitate encryption and decryption operations of objects. [Amazon RDS](#) also supports Transparent Data Encryption (TDE).

It is possible to encrypt data on Linux Amazon EC2 instance stores by using built-in Linux or Microsoft libraries. This method encrypts files transparently, which protects confidential data. As a result, applications that process the data are unaware of the disk-level encryption.

You can use two methods to encrypt files on instance stores:

- **Disk-level encryption** — With this method, the entire disk, or a block within the disk, is encrypted using one or more encryption keys. Disk encryption operates below the file system level, is operating-system agnostic, and hides directory and file information, such as name and size. Encrypting File System, for example, is a Microsoft extension to the Windows NT operating system's New Technology File System (NTFS) that provides disk encryption.
- **File system-level encryption** — With this method, files and directories are encrypted, but not the entire disk or partition. File-system-level encryption operates on top of the file system and is portable across operating systems.

For Non-Volatile Memory express (NVMe) SSD instance store volumes, disk-level encryption is the default option. Data in an NVMe instance storage is encrypted using an XTS-AES-256 block cipher implemented in a hardware module on the instance. The encryption keys are generated using the hardware module and are unique to each NVMe instance storage device. All encryption keys are destroyed when the instance is stopped or terminated and cannot be recovered. You cannot use your own encryption keys.

Encrypt Data in Transit

AWS strongly recommends encrypting data in transit from one system to another, including resources within and outside of AWS.

When you create an AWS account, a logically isolated section of the AWS Cloud—the [Amazon Virtual Private Cloud](#) (Amazon VPC)—is provisioned to it. There, you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selecting your own IP address range, creation of subnets, and configuration

of route tables and network gateways. You can also create a hardware Virtual Private Network (VPN) connection between your corporate datacenter and your Amazon VPC, so you can use the AWS Cloud as an extension of your corporate datacenter.

For protecting communication between your Amazon VPC and your corporate datacenter, you can select from several VPN connectivity options, and choose one that best matches your needs. You can use the [AWS Client VPN](#) to enable secure access to your AWS resources using client-based VPN services. You can also use a third-party software VPN appliance available in the AWS Marketplace, which you can install on an Amazon EC2 instance in your Amazon VPC. Alternatively, you can create an IPsec VPN connection to protect the communication between your VPC and your remote network. To create a dedicated private connection from a remote network to your Amazon VPC, you can use [AWS Direct Connect](#). You can combine this connection with an AWS Site-to-Site VPN to create an IPsec-encrypted private connection.

AWS provides HTTPS endpoints using the TLS protocol for communication, which provides encryption in transit when you use AWS APIs. You can use the [AWS Certificate Manager](#) (ACM) service to generate, manage, and deploy the private and public certificates you use to establish encrypted transport between systems for your workloads. Elastic Load Balancing is integrated with ACM and is used to support HTTPS protocols. If your content is distributed through Amazon CloudFront, it supports encrypted endpoints.

Encryption Tools

AWS offers various highly scalable data encryption services, tools, and mechanisms to help protect your data stored and processed on AWS. For information about AWS Service functionality and privacy, refer to [Privacy Features of AWS services](#).

Cryptographic services from AWS use a wide range of encryption and storage technologies that are designed to maintain integrity of your data at rest or in transit. AWS offers four primary tools for cryptographic operations.

- [AWS Key Management Service](#) (AWS KMS) is an AWS managed service that generates and manages both root keys and data keys. AWS KMS is integrated with many AWS services to provide server-side encryption of data using AWS KMS keys from customer accounts. AWS KMS Hardware Security Modules (HSMs) are FIPS 140-2 Level 3 validated. In November 2022, AWS announced the availability of AWS Key Management Service (AWS KMS) External Key Store. Customers who have a regulatory need to store and use their encryption keys on premises or outside of the AWS Cloud can now do so. This capability allows you to store AWS KMS customer

managed keys on a hardware security module (HSM) that you operate on-premises or at any location of your choice. KMS External Key Stores (XKS) allow you to protect your AWS resources using cryptographic keys stored in an external key management system that you control. External key stores support the AWS digital sovereignty pledge to give you sovereign control over your data in AWS, including the ability to encrypt with key material that you own and control outside of AWS.

- AWS CloudHSM provides HSMs that are FIPS 140-2 Level 3 validated. They securely store a variety of your self-managed cryptographic keys, including KMS keys and data keys.
- AWS Cryptographic Services and Tools
- [AWS Encryption SDK](#) is a client-side encryption library designed to make it easy for everyone to encrypt and decrypt data using industry standards and best practices. It enables you to focus on the core functionality of your application, rather than on how to best encrypt and decrypt your data.
- [AWS Database Encryption SDK](#) is a set of software libraries that enable you to include client-side encryption in your database design. The AWS Database Encryption SDK provides record-level encryption solutions. You specify which fields are encrypted and which fields are included in the signatures that ensure the authenticity of your data. Encrypting your sensitive data in transit and at rest helps ensure that your plaintext data isn't available to any third party, including AWS.

AWS Key Management Service

[AWS Key Management Service](#) (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS KMS is integrated with several other AWS services to help you protect the data you store with these services. AWS KMS is also integrated with AWS CloudTrail to provide you with logs of all your key usage for your regulatory and compliance needs.

AWS KMS supports several different types of keys for different uses and the several special purpose KMS key types including key with imported key material (BYOK) and key in a custom key store, that is backed by an AWS CloudHSM cluster or an external key manager outside of AWS.

You can easily create, import, and rotate keys, as well as define usage policies and audit usage from the AWS Management Console or by using the AWS SDK or AWS CLI.

The AWS KMS Keys in AWS KMS, whether imported by you or created on your behalf by KMS, are stored in highly durable storage in an encrypted format to help ensure that they can be used when

needed. You can choose to have KMS automatically rotate AWS KMS Keys created in KMS once per year without having to re-encrypt data that has already been encrypted with your KMS key. You don't need to keep track of older versions of your AWS KMS Keys because KMS keeps them available to automatically decrypt previously encrypted data.

For any AWS KMS Key in AWS KMS, you can control who has access to those keys and which services they can be used with through a number of access controls, including grants, and key policy conditions within key policies or IAM policies. You can also import keys from your own key management infrastructure and use them in KMS.

For example, the following policy uses the `kms:ViaService` condition to allow a customer managed AWS KMS Key to be used for the specified actions only when the request comes from Amazon EC2 or Amazon RDS in a specific Region (`us-west-2`) on behalf of a specific user (`ExampleUser`).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
      }
      "Action": [
        "kms:Encrypt*",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "kms:ViaService": [
            "ec2.us-west-2.amazonaws.com",
            "rds.us-west-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS Service Integration

AWS KMS has integrated with a number of AWS services – refer to the [KMS website](#) for a full list of integrated services. These integrations enable you to easily use AWS KMS Keys to encrypt the data you store with these services. In addition to using a customer managed AWS KMS Key, a number of the integrated services enable you to use an AWS-managed AWS KMS Key that is created and managed for you automatically, but is only usable within the specific service that created it.

Audit Capabilities

[AWS CloudTrail](#) records each use of a key that you store in AWS KMS in a log file that is delivered to the Amazon S3 bucket that you specified in your configuration of CloudTrail. The information recorded includes details of the user, time, date, operation performed, and the key used.

Security

AWS KMS is designed to make sure that no one has access to your KMS keys. The service is built on systems that are designed to protect your KMS keys with extensive hardening techniques, such as never storing plaintext KMS keys on disk, not persisting them in memory, and limiting which systems can access hosts that use keys. All access to update software on the service is controlled by a multi-party access control that is audited and reviewed by an independent group within AWS.

For more information about AWS KMS, see the [AWS Key Management Service whitepaper](#).

AWS CloudHSM

The [AWS CloudHSM](#) is a cloud-based hardware security module (HSM) that helps you meet corporate, contractual, and regulatory compliance requirements for data security by enabling you to generate and use your encryption keys on a FIPS 140-2 Level 3 validated hardware.

With AWS CloudHSM, you control the encryption keys and cryptographic operations performed by HSM.

This is designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption to make sure that only you can get access to them. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance.

The AWS CloudHSM service works with Amazon VPC. AWS CloudHSM instances are provisioned inside your Amazon VPC with an IP address that you specify, which provides simple and private network connectivity to your Amazon EC2 instances. When you locate your HSM instances

near your Amazon EC2 instances, you decrease network latency, which can improve application performance. AWS provides dedicated and exclusive (single tenant) access to HSM instances, which are isolated from other customers. Available in multiple Regions and Availability Zones, AWS CloudHSM enables you to add secure and durable key storage to your applications.

Integration with AWS Services and Third-Party Applications

You can use CloudHSM with [Amazon Redshift](#), [Amazon RDS](#) for Oracle, or third-party applications (such as SafeNet Virtual KeySecure) as your Root of Trust, Apache (SSL termination), or Microsoft SQL Server (transparent data encryption). You can also use AWS CloudHSM when you write your own applications and continue to use the standard cryptographic libraries, including PKCS#11, Java JCA/JCE, and Microsoft CAPI and CNG.

Audit Activities

If you need to track resource changes, or audit activities for security and compliance purposes, you can review the management API calls over the AWS CloudHSM made from your account using [AWS CloudTrail](#). Additionally, you can audit operations on the HSM appliance using syslog or send syslog log messages to your own log collector.

AWS Cryptographic Services and Tools

AWS offers mechanisms that comply with a wide range of cryptographic security standards that you can use to implement best-practice encryption. The [AWS Encryption SDK](#) is a client-side encryption library, available in Java, Python, C, JavaScript, and a command line interface that supports Linux, macOS, and Windows. It offers advanced data protection features including secure, authenticated, symmetric key algorithm suites, such as 256-bit AES-GCM with key derivation and signing. Because it was specifically designed for applications that use [Amazon DynamoDB](#), the DynamoDB Encryption Client enables users to protect their table data before it is sent to the database. It also verifies and decrypts data when it is retrieved. The client is available in Java and Python.

Linux DM-Crypt Infrastructure

Dm-crypt is a Linux kernel-level encryption mechanism that allows users to mount an encrypted file system. Mounting a file system is the process in which a file system is attached to a directory (mount point), which makes it available to the operating system. After mounting, all files in the file system are available to applications without any additional interaction. These files are, however, encrypted when stored on disk.

Device mapper is an infrastructure in the Linux 2.6 and 3.x kernel that provides a generic method to create virtual layers of block devices. The device mapper crypt target provides transparent encryption of block devices using the kernel crypto API. The solution in this post uses dm-crypt in conjunction with a disk-backed file system mapped to a logical volume by the Logical Volume Manager (LVM). LVM provides logical volume management for the Linux kernel.

Client-side Encryption

Client-side encryption provides an additional layer of data protection by encrypting data before it is sent to AWS. This approach ensures that the data is encrypted at its source and remains encrypted throughout its lifecycle in the cloud, reducing the risk of unauthorized access during transmission and storage. AWS provides several tools and libraries to facilitate client-side encryption. The AWS Encryption SDK, available in multiple programming languages including Java, Python, C, and JavaScript, offers a framework for implementing envelope encryption with support for AWS KMS for key management. For Amazon S3 specifically, the [Amazon S3 Encryption Client](#) enables easy implementation of client-side encryption for S3 objects. When using [Amazon DynamoDB](#), the [AWS Database Encryption SDK](#) allows for client-side encryption of table data before it's sent to the database. These tools support both symmetric and asymmetric encryption algorithms and can be integrated with AWS KMS for enhanced key management. By implementing client-side encryption, customers maintain full control over their encryption keys and can ensure that their most sensitive data is never exposed in plaintext outside their own environments. This approach can be particularly valuable for customers with stringent data protection requirements or those looking to implement an additional safeguard for highly sensitive personal data under the GDPR.

Post-Quantum Cryptography

AWS's encryption tools and services are evolving to address the emerging challenges of quantum computing and its potential impact on current cryptographic methods. AWS KMS supports hybrid post-quantum TLS, which combines traditional and quantum-resistant algorithms to help protect data in transit from both current and future threats. This capability is particularly relevant for data that must remain confidential over extended periods, as required by the GDPR's security principles. For implementation, AWS provides the s2n-tls library, which includes hybrid post-quantum key exchange algorithms that are being evaluated as part of NIST's Post-Quantum Cryptography standardization process. The [AWS Encryption SDK](#) is designed with crypto-agility in mind, allowing for the integration of post-quantum algorithms as they become standardized. [AWS Certificate Manager's](#) integration with hybrid post-quantum TLS enables customers to prepare their applications for the post-quantum era while maintaining backward compatibility. These tools

support AWS's quantum-safe strategy, which includes the principle of crypto-agility – designing systems that can smoothly transition to new cryptographic algorithms as they become necessary. Customers can use AWS CloudTrail to audit their use of cryptographic operations and AWS Config to track their cryptographic configurations, helping them prepare for and manage the eventual transition to post-quantum cryptography while maintaining continuous compliance with data protection requirements.

Pseudonymization

AWS provides several approaches and services to help customers implement pseudonymization of personal data. AWS KMS can be used with [AWS Encryption SDK](#) to create and manage data keys for encrypting specific data fields, while maintaining separate mapping of original values. [Amazon DynamoDB](#) supports attribute encryption for specific fields, enabling selective pseudonymization of personal data within database records. For application-level pseudonymization, [AWS Lambda](#) can be used to create serverless functions that transform data during processing or API calls. [AWS Glue](#) provides capabilities for data transformation during ETL processes, including the ability to mask or tokenize sensitive fields.

For customers requiring more specialized solutions, [AWS Marketplace](#) offers various third-party tools such as Protegrity Data Protection Platform, TokenEx Cloud Data Protection, and the Privacera Data Security Platform, which provide advanced data masking, tokenization, and pseudonymization capabilities. These solutions integrate with AWS services and can be deployed across multiple AWS accounts and regions.

When implementing pseudonymization, customers can use [AWS CloudTrail](#) for auditing all pseudonymization operations and [AWS Secrets Manager](#) to securely store and manage the mapping keys or transformation rules required for re-identification.

Data Protection by Design and by Default

[AWS Nitro System](#) is the underlying platform for all modern Amazon EC2 instances. It is a combination of purpose-built server designs, data processors, system management components, and specialized firmware which provide the underlying platform for all Amazon EC2 instances launched since the beginning of 2018. By design the Nitro System has no operator access; it means that there is no mechanism for any system or person to log in to Amazon EC2 Nitro hosts, access the memory of Amazon EC2 instances, or access any customer data stored on local encrypted instance storage or remote encrypted Amazon EBS volumes. If any AWS operator, including those

with the highest privileges, needs to do maintenance work on an Amazon EC2 server, they can only use a limited set of authenticated, authorized, logged, and audited administrative APIs. None of these APIs provide an operator the ability to access customer data on the Amazon EC2 server. Because these are designed and tested technical restrictions built into the Nitro System itself, no AWS operator can bypass these controls and protections. This is also reflected in the [AWS Service Terms](#) clause on AWS Nitro System which includes “There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access Your Content on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance”. You can find additional details about Nitro System's security design and the independent affirmation of these security capabilities from NCC Group, a leading cybersecurity consulting firm, in the public documentation (see [AWS Nitro System](#), [The Security Design of the AWS Nitro System](#), [AWS Nitro System gets independent affirmation of its confidential compute capabilities](#)).

Additionally, any time a user or an application tries to use the AWS Management Console, the AWS API, or the AWS CLI, a request is sent to AWS. The AWS service receives the request and executes a set of several steps to determine whether to allow or deny the request, according to a specific policy evaluation logic. Except for root credential requests, all requests on AWS are denied by default (the default deny policy is applied). This means that everything that is not explicitly allowed by the policy is denied. In the definition of policies and as a best practice, AWS suggests that you apply the least privilege principle.

This approach aligns with Article 25 of the GDPR, which states that “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”.

AWS also provides tools to implement infrastructure as code, which is a powerful mechanism for including security from the beginning of the design of an architecture. [AWS CloudFormation](#) provides a common language to describe and provision all infrastructure resources, including security policies and processes. With these tools and practices, security becomes part of your code and can be versioned, monitored, and modified (with a versioning system) according to the requirements of your organization. This enables data protection by design, because security processes and policies can be included in the definition of your architecture and can also be continuously monitored by security measures in your organization.

AWS Nitro Enclaves

[AWS Nitro Enclaves](#) enhances AWS's data protection by design capabilities by providing an isolated compute environment that helps customers process highly sensitive data with an additional layer

of security. Nitro Enclaves are isolated virtual machines that are created from Amazon EC2 instance resources but remain completely isolated from the parent instance, other applications, and the cloud provider itself. This isolation is enforced through the [AWS Nitro System's](#) hardware-based security and attestation. When processing personal data under the GDPR, Enclaves provide a trusted execution environment where sensitive operations like encryption, decryption, or data tokenization can be performed in complete isolation. The Enclaves' cryptographic attestation model ensures that only authorized code can run within the Enclave and access sensitive data or cryptographic keys. Integration with AWS KMS allows Enclaves to use special encryption keys that can only be accessed from within a properly attested Enclave, providing an additional control for protecting sensitive data processing operations. This capability is particularly valuable for applications handling special categories of personal data under the GDPR, or for implementing privacy-preserving computing solutions where data must remain encrypted throughout its lifecycle. Nitro Enclaves support the principle of data protection by design by providing a verifiable, isolated environment for sensitive data processing that's built into the infrastructure level.

How AWS Can Help

Table 1 – How AWS can help you navigate GDPR compliance

Area	Description	AWS Services and Tools
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.”	<p>The framework is validated by following certifications and attestations:</p> <p>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 / ISO 27701 NIST FIPS 140-2 Cloud Computing Compliance Criteria Catalog (C5)</p>
Data Access Control	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.”	<p>AWS Identity and Access Management (IAM)</p> <p>Amazon Cognito</p> <p>AWS Shield and AWS WAF</p> <p>AWS Resource Access Manager</p> <p>Amazon CloudFront</p> <p>AWS Organizations</p> <p>AWS CloudTrail</p>
Monitoring, Logging and Records of Processing	“Each controller and, where applicable, the controller’s representative, shall maintain a record of processing	<p>AWS Config</p> <p>Amazon CloudWatch</p>

Area	Description	AWS Services and Tools
	<p>activities under its responsibility." "...the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk [...]"</p>	<p>AWS Control Tower</p> <p>Amazon GuardDuty</p> <p>Amazon Detective</p> <p>Amazon Inspector</p> <p>Amazon Macie</p> <p>AWS Systems Manager</p> <p>AWS Security Hub</p> <p>AWS Security Lake</p> <p>Amazon Security Lake</p> <p>AWS Tools and SDKs</p>
<p>Protecting your Data on AWS</p>	<p>Organizations must "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including [...] the pseudonymization and encryption of personal data."</p>	<p>AWS Certificate Manager</p> <p>AWS CloudHSM</p> <p>AWS Nitro Systems</p>

Area	Description	AWS Services and Tools
Data Protection Impact Assessment (DPIA)	AWS provides services and resources that assist customers in completing their DPIA when using AWS services. The GDPR determines the customer is responsible for determining if a DPIA is required, for choosing an assessment methodology, and for performing the assessment.	<p>AWS Service Terms</p> <p>AWS Artifact</p> <p>AWS Compliance Programs</p>
Data Transfer Impact Assessment (DTIA)	The Annex to this whitepaper provides more information for customers that want to perform an assessment on data transfers when using AWS services.	<p>AWS Service Terms</p> <p>AWS Privacy Features</p> <p>AWS Sub-Processors webpages</p>
PII Data Discovery	Organizations must identify and classify personal data to implement appropriate protection measures and demonstrate GDPR compliance. AWS provides tools to automatically discover, classify, and monitor personal data across AWS services.	<p>Amazon Macie for automated sensitive data discovery and classification</p> <p>AWS Glue Data Catalog for data inventory and classification</p> <p>Amazon EMR for large-scale data processing and analysis</p> <p>AWS CloudWatch Logs pattern matching for log analysis</p>

Contributors

Contributors to this document include:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Senior Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect Manager, Amazon Web Services

Document history

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Minor Update	Updated content to reflect current service names and features.	February 19, 2026
Minor update	Updated content. Integration of data transfer guidance as new Annex	May 11, 2025
Minor update	Updated references to latest DPA.	November 2, 2023
Minor update	Fix non-inclusive language.	April 6, 2022
Minor update	Updated to include the addition of new AWS services and functionalities.	December 1, 2020
Initial publication	Whitepaper first published.	November 1, 2017

Note

Note: To subscribe to RSS updates, you must have an RSS plug-in enabled for the browser that you are using.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2026 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Annex: AWS Customer EU Data Transfer Assessment Guide

AWS is committed to enabling customers to use all AWS services. This Annex provides customers with information to assist them in using AWS services in compliance with the quickly evolving data protection landscape, specifically in accordance with recommendations from the European Data Protection Board (EDPB) (Recommendations 01/2020), and conducting their data transfer assessment(s) (DTAs). If a customer does not use AWS services that involve the transfer of customer data outside the European Economic Area (EEA), the United Kingdom or Switzerland, carrying out a DTA with regard to its use of AWS might not be required.

This DTA Annex describes the key supplementary measures taken by AWS and made available to customers by AWS to enable each customer to protect personal data subject to the GDPR (including to assist a customer with meeting its DTA obligations) that has been uploaded to the AWS services under its AWS accounts (customer data).

Data Transfer Assessment Information

The following sections provide customers with information to assist in conducting a DTA. Since AWS does not know what content customers upload to AWS services, customers need to evaluate the details of their processing, taking into account how they are using AWS services, to prepare their DTA. In order to provide customers with the most helpful information for their DTA, the sections have been structured according to the instructions for completing DTAs set out in the EDPB Recommendations, which recommend that data exporters perform the following six-step data transfer assessment (the EDPB data transfer assessment):

- Step 1: Know your transfers
- Step 2: Identification of transfer tools relied on
- Step 3: Assessment of applicable laws and practices in relevant countries
- Step 4: Adoption of supplementary measures (if required)
- Step 5: Procedural steps for supplementary measures
- Step 6: Re-evaluation

In summary

- The customer selects the AWS region in which it stores its customer data. In accordance with the [AWS Data Processing Addendum](#) (AWS DPA), AWS will not transfer customer data outside the customer's selected AWS region unless it is necessary to provide or maintain the AWS services initiated by the customer, or as necessary to comply with the law or a valid and binding order.
- Where the customer instructs the AWS services to transfer customer data to third countries, AWS uses the SCCs as a data transfer tool under Chapter V of the GDPR to validate such transfers (unless AWS has adopted an alternative recognized compliance standard for lawful data transfers). The SCCs are part of the [AWS Service Terms](#), are incorporated by reference into the [AWS DPA](#), and apply automatically in case of a data transfer.
- AWS takes and makes available additional technical, organizational, and contractual supplementary measures to protect customer data and supplement the SCCs.

In detail

STEP 1: KNOW YOUR TRANSFERS

Customers need to understand whether their use of AWS services may lead to a data transfer, and if so, what customer data is transferred in order to be able to fulfil their obligations under the GDPR's principle of accountability. As a first step, the customer, therefore, needs to identify which data transfers might take place in connection with its use of AWS services.

The customer determines which AWS services it uses, or intends to use, and what customer data it processes and for which purposes when using the AWS services. Due to the content-agnostic nature of the AWS services, AWS does not have visibility into customer data. Therefore, only the customer can complete this step 1, based on where and how it chooses to use AWS services.

AWS's European seller of record (Amazon Web Services EMEA SARL), based in Luxembourg, is the AWS contracting party that provides AWS services to customers who have AWS accounts associated with Europe, the Middle East and Africa (other than South Africa). As set out in the [AWS Customer Agreement](#), other AWS affiliates provide the AWS services to customers located outside of Europe, the Middle East and Africa.

As set out in the [AWS DPA](#), AWS will not transfer customer data outside the customer's selected AWS region unless it is necessary to provide or maintain the AWS services initiated by the customer, or as necessary to comply with the law or a valid and binding order.

The theoretical possibility of a governmental body in a third country being permitted by law to order the transfer of customer data in response to a disclosure request does not constitute a data transfer. This has been confirmed by data protection authorities, for example the German data protection authorities as well as German courts and procurement chambers. Nevertheless, the customer may use the information described in step 4 below, to implement technical and organizational measures to protect customer data in compliance with the GDPR.

The following bullet points provide customers with more details on typical processing activities carried out by AWS in connection with customers' use of AWS services. This information could be used by customers to assist them in completing their DTA, subject to appropriate customization based on their business activities and unique use of AWS services:

Description of the transfer of customer data, including relevant sub-processors

- The customer may select from a suite of on-demand AWS services that customers

can configure to build its own products and service offerings. Customers maintain control over their customer data at all times, through tools that enable customers to determine where customer data will be stored and to secure customer data in transit and at rest.

- The customer selects the AWS region(s) to store its customer data in accordance with the [AWS DPA](#). Customers can use AWS regions in Europe, including France, Germany, Ireland, Italy, Spain, Sweden, Switzerland, and the UK. The [Regions and Availability Zones website](#) provides a full overview of the AWS regions.
- AWS will not transfer customer data outside the customer's selected AWS region unless it is necessary to provide the AWS services initiated by the customer, or as necessary to comply with law or a valid and binding order, or where it is required in order to prevent fraud and abuse.
- As a general rule, the customer can use AWS services with the confidence that customer data stays in the AWS region(s) that the customer selects and a data transfer is not required to provide or maintain the services. Only a small number of AWS services involve transfers of customer data to countries outside the AWS region selected by the customer which may include third countries. Customers can find an overview of such AWS services (e.g., content delivery services) on the [AWS Privacy Features page](#). In few cases, AWS uses customer data to develop and improve the respective service

which involves data transfers. Customers can opt-out from such data transfers as described in the [AWS Service Terms](#). A list of the AWS services that allow for an opt-out on data transfers can be found on the [Privacy Features page](#). Alternatively, customers can implement policies to avoid use of such AWS services.

- On the [AWS Sub-processors website](#), customers can learn more about the sub-processors that provide processing activities on customer data, including the AWS entity acting as sub-processor in their chosen AWS region (e.g., A 100 ROW GmbH for AWS Region: Europe (Frankfurt)). The [AWS Sub-processors website](#) lists the location of each sub-processor. There are three types of sub-processors: (1) AWS entities that provide the infrastructure on which the AWS services run; (2) AWS entities that support specific AWS services which may require these entities to process customer data; and (3) third parties that AWS has contracted with to provide processing activities for specific AWS services. The second type of sub-processors includes AWS entities that provide AWS Support services, but these entities do not process customer data unless the customer wants to share customer data in the course of requesting AWS Support (which AWS does neither require nor recommend). AWS will update the [AWS Sub-processors website](#) at least 30 days before engaging a new sub-processor, and if customers [subscribe](#) for updates, AWS will notify them by email of changes to this

	<p>website. The AWS Sub-processors website also lists the Amazon entities that are used to provide customer-initiated support.</p> <ul style="list-style-type: none"> • These entities do not process customer data unless the customer chooses to share customer data in the course of requesting AWS Support (which AWS neither requires nor recommends). As an example, AWS Support may process customer data if the customer shares its screen or attaches a snapshot to the ticket.
<p>Processing activity</p>	<ul style="list-style-type: none"> • Compute, storage, and such other AWS services as described for each AWS service in the Documentation and initiated by the customer from time to time. The customer decides on the exact processing activity.
<p>Purpose for which customer data are transferred</p>	<ul style="list-style-type: none"> • The customer decides on the purposes for which customer data is transferred (if at all) as transfers (if any) occur based on the customer’s selection of AWS services and AWS regions.
<p>Categories of customer data concerned</p>	<ul style="list-style-type: none"> • The customer controls the categories of customer data it uploads to the AWS services. Customers are free to upload any category of customer data to the AWS services, which may include for instance data in relation to purchase contracts, employment relationships, or analytics data.
<p>Data minimization</p>	<ul style="list-style-type: none"> • The customer controls how to address data minimization obligations and measures in the context of transfers of customer data.

<p>Categories of data subjects concerned</p>	<ul style="list-style-type: none"> • The customer controls the categories of data subjects whose personal data is uploaded to AWS services. The data subjects may include, for example, the customer’s customers, employees, suppliers, and end users.
<p>Actors involved in the processing (including sub-processors); processing chain</p>	<ul style="list-style-type: none"> • Customers might be controllers or processor s of customer data, depending on the role and responsibilities they take in respect of their data processing activities. • AWS is always a processor of customer data and carries out any processing on behalf of the customer. Each customer contracts with an AWS contracting party that provides the AWS services depending on the location associated with the customer’s account. For customers with accounts located in the EEA, the AWS contracting party that provides the AWS services to customers is Amazon Web Services EMEA SARL, based in Luxembourg. In case of a data transfer, Amazon Web Services, Inc. acts as data importer under the SCCs. • Customers may learn about the sub-proce ssors that may be relevant to their selected AWS services on the AWS Sub-processor website.
<p>Economic sector in which transfers of customer data occur</p>	<ul style="list-style-type: none"> • Customers operate in various economic sectors and use the AWS services for a broad range of use cases. Accordingly, the economic sector in which data transfers of customer data occur depend on the customer’s business activities.

Format of transferred customer data

- The customer controls the format of transferred customer data. Customers can elect to use technical measures affecting the format in order to protect customer data. For example, most AWS services enable customers to encrypt customer data, as shown on the [Privacy Features of AWS page](#), or with customers' own or selected third-party technologies.

Volume and frequency of transfer of customer data

- The customer determines the volume of customer data transferred and how frequently it transfers customer data based on the AWS services that the customer selects, and the customer's architecture and configuration of those AWS services.

Security measures to protect customer data

- AWS's [Shared Responsibility Model](#) distinguishes between the responsibility for what AWS calls "Security OF the Cloud" on the one hand and "Security IN the Cloud" on the other hand. While AWS is responsible for the "Security OF the Cloud", each customer is responsible for "Security IN the Cloud. For "Security OF the Cloud", AWS implements technical and physical controls and processes designed to prevent unauthorized access or disclosure of customer data (as evidenced by its compliance program detailed on the [AWS Compliance website](#)). For "Security IN the Cloud", AWS makes available products, tools, and services that customers can use to architect and secure their applications and solutions. Customers can refer to the [AWS Well-Architected website](#) for further information about such products, tools, and services. Additionally, customers can implement and use their own or third-party security tools (e.g., purchased on the AWS marketplace) in connection with the AWS services.
- AWS prohibits, and its systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by a customer, is required to prevent fraud and abuse, or to comply with law.
- AWS maintains access controls and policies to limit, manage, and control the access of AWS personnel to customer data, including the use of firewalls or functionally equivalent technology and authentication controls in

accordance with the AWS Security Standards (included in the [AWS DPA](#)).

- AWS adheres to the [Cloud Infrastructure Service Providers Europe \(CISPE\) Data Protection Code of Conduct \(CISPE Code\)](#) validated by the EDPB and approved by the French Data Protection Authority (CNIL). The CISPE Code assures organizations that their cloud infrastructure service provider meets the requirements applicable to customer data under the GDPR. The CISPE Code goes beyond compliance with the GDPR by requiring cloud infrastructure service providers to give customers the choice to use services to store and process customer data exclusively in the EEA. AWS has initially declared 100 services under the CISPE Code and is committed to bringing additional AWS services into the scope of the CISPE compliance program. For further information, see [AWS cloud services adhere to CISPE Data Protection Code of Conduct for added GDPR assurance](#).

STEP 2: IDENTIFY THE TRANSFER TOOLS YOU ARE RELYING ON

If a customer has determined in step 1 of its DTA that its use of AWS services leads to an international data transfer, the customer must identify and document in step 2 of its DTA the transfer tool it is relying on as a lawful basis for the data transfer pursuant to chapter V of the GDPR. A customer might also choose to use a transfer tool other than an adequacy decision as the lawful basis for a transfer of personal data to a country that has received an adequacy decision from the European Commission, which would also need to be documented in step 2 of its DTA.

Transfer tool:

- The SCCs apply to the international data transfer that the customer has determined to take place in step 1 of this DTA. The SCCs are part of the [AWS Service Terms](#) and incorporated by

reference into the [AWS DPA](#). Although the SCCs are already part of a customer's contract with AWS, they only apply if the customer's use of AWS services involves a data transfer to a country not recognized by the European Commission as providing an adequate level of protection for personal data subject to GDPR.

- Both the [Controller-to-Processor Clauses](#) and the [Processor-to-Processor Clauses](#) are incorporated into the [AWS DPA](#), and apply as appropriate depending on whether the customer is a controller or a processor. The [Controller-to-Processor Clauses](#) apply to data transfers when customers are controllers, and the [Processor-to-Processor Clauses](#) apply to data transfers where customers are processors. See our blog post [New Standard Contractual Clauses now part of the AWS GDPR Data Processing Addendum for customers](#) for further information.
- AWS enters into appropriate standard contractual clauses with its sub-processors to validate onward transfers.
- AWS offers additional addenda supplementing the DPA for data transfers from the [United Kingdom](#) and [Switzerland](#) to third countries (as defined under each country's data protection law).

STEP 3: ASSESS THE LAWS OR PRACTICES OF THE COUNTRIES THAT MAY IMPINGE ON THE EFFECTIVENESS OF THE TRANSFER TOOL

In step 3 of its DTA, a customer needs to assess whether the transfer tool that it relies on for data transfers in step 2 of its DTA is effective in ensuring that the level of protection guaranteed by the GDPR is not undermined by the laws and practices in the country to which its customer data is transferred.

Only the customer controls if and where its customer data is transferred in connection with its use of its selected AWS services. When assessing the risk in connection with the processing of customer data in a particular country, several factors might be relevant that only the customer can control, e.g., the sensitivity of the processed data categories, the purposes for which the customer uses the AWS services, or whether the customer's business has ties to that country. This will be relevant for a customer when determining whether its customer data will receive protection in a country that is equivalent to the GDPR. A customer might, therefore, wish to conduct a review of certain countries that are relevant to its specific use of AWS services when completing this step of its DTA.

The supplementary measures AWS takes and makes available to its customers – described in step 4 below – including AWS's approach towards governmental disclosure requests, apply globally. AWS is confident that these measures set a high threshold to protect customer data against unwanted

or unauthorized access or disclosure regardless of the specific jurisdiction in which customer data may be processed due to customer's specific use of the AWS services. A customer might still wish to map these supplementary measures against the specific framework of a particular country that is relevant for that customer. When assessing relevant laws, a customer should first check the data transfer position determined in step 1 of its DTA and review it against the legal framework and practices applicable in the relevant countries.

For example, for transfers of customer data to the US, on July 10, 2023, the European Commission adopted its adequacy decision on the DPF. The decision, which took effect on the day of its adoption, concludes that the US ensures an adequate level of protection for personal data transferred from the EEA to companies certified to the DPF. The European Commission also confirmed that safeguards that have been implemented as part of the DPF "facilitate the use of other tools, such as standard contractual clauses and binding corporate rules". When relying on SCCs for transfers of customer data to the US and conducting a DTA, customers can consider the European Commission's adequacy decision that finds that the safeguards under the DPF provide a level of protection essentially equivalent to the protection afforded under the GDPR.

The following additional resources might also be helpful to assist a customer when completing step 3 of its DTA:

- Factsheet of the ECtHR jurisprudence on mass surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
- Country reports of the Inter-American Commission on Human Rights (IACHR): <https://www.oas.org/en/iachr/reports/country.asp>
- Global Privacy Assembly – Global Frameworks and Standards Report: https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf
- United Nations Human Rights Council Documentation by country: <https://www.ohchr.org/en/hr-bodies/upr/documentation>
- United Nations Human Rights Treaty Bodies – UN Treaty Body Database: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

Irrespective of the laws that apply and regardless of the country from which it originates, AWS reviews every law enforcement request it may receive individually and independently. AWS challenges government requests for customer information, including customer data, that it believes are or could be overbroad or otherwise inappropriate. AWS thoroughly scrutinizes such

requests, including those that conflict with local law, such as the GDPR, and objects where it has appropriate grounds to do so. AWS also takes and makes available supplementary measures, including contractual commitments, to support the effectiveness of the SCCs, as described in step 4 below.

The EDPB's recommendations also permit customers to consider AWS's practical experience "with relevant prior instances of requests for access received from public authorities" outside of the EEA. AWS publishes regular [Amazon Information Request Reports](#), which detail the types and volume of law enforcement requests that AWS receives, which are available for customers to review. The contents of the information request reports demonstrate that disclosures of customer data by AWS in response to government requests for information are very rare.

STEP 4: ADOPT SUPPLEMENTARY MEASURES IF REQUIRED

In step 4 of its DTA, a customer might identify supplementary measures that can be taken if the assessment in step 3 of its DTA reveals that the relevant proposed data transfer tool on its own does not provide effective protection for customer data as required by the GDPR.

The SCCs in place between AWS and its customers are effective in ensuring an essentially equivalent level of data protection. In addition, AWS also offers effective technical, organizational, and contractual measures to ensure an equivalent level of protection for customer data that is transferred outside of the EEA, UK, and Switzerland.

The following categories of supplementary measures are implemented or offered to customers for implementation: (a) **technical measures**, such as encryption and logging, implementation of policies that are technically enforced to avoid the use of AWS services involving data transfers; (b) **organizational measures**, comprising internal policies and standards regarding governmental requests for customer data; and (c) **contractual protections**, including commitments with respect to law enforcement requests for customer data like those AWS makes in the [AWS Supplementary Addendum](#).

AWS operates the Shared Responsibility Model described in step 1 above, which apportions security and compliance responsibilities between AWS and its customers based on the way AWS services operate and the degree of control each party has. Under the Shared Responsibility Model, it is the customer's responsibility to implement the technical and organizational measures required in connection with its DTA.

Technical supplementary measures

The following supplementary measures are made available by AWS to customers to assist with safeguarding data transfers:

Encryption

AWS provides advanced encryption services and tools that customers can use to protect their customer data.

Customers can use AWS's Key Management Service (AWS KMS) as a managed service in the AWS environment. AWS KMS allows customers to create and control their encryption keys, and uses FIPS- 140-2 certified Hardware Security Modules (HSM) to protect the security of such keys. All requests to use keys in AWS KMS are logged in AWS CloudTrail so customers can understand who used which key, in what context, and when it was used. Event data logged to AWS CloudTrail cannot be altered. AWS KMS is designed so that neither AWS (including AWS employees) nor third-party providers to AWS can retrieve, view, or disclose customer's master keys in an unencrypted format.

Customers can manage their own encryption keys (BYOK) from within a number of native AWS or third-party encryption solutions. For example, customers can also use the External Key Store (XKS) feature of AWS KMS or their own external key stores allowing them to protect their AWS resources using cryptographic keys outside of AWS. An external key store is a [custom key store](#) backed by an external key manager that customers own and manage outside of AWS.

For more information, see the AWS KMS FAQs [here](#).

AWS Nitro System

The AWS Nitro System is the underlying platform for all modern Amazon Elastic Compute Cloud (EC2) instances, and it provides additional confidentiality and privacy for customers' applications. Using purpose-built hardware, firmware, and software, the AWS Nitro System provides unique and industry-leading security and isolation by offloading virtualization functions, like storage and networking, to dedicated hardware and associated firmware. As AWS commits in the [AWS Service Terms](#), AWS personnel do not have access to customer data on AWS Nitro System EC2 instances. There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access customer data on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance. NCC Group, a global cybersecurity consulting firm, conducted an architecture review of our security claims of the Nitro System and our claims about operator access. In its report NCC Group confirms that the AWS Nitro System, by design, has no mechanism for anyone at AWS to access customer data on Nitro hosts.

For more information, see the [Security Design of the AWS Nitro System Whitepaper](#) and our [blog post](#).

Organizational supplementary measures

Processes

AWS has internal processes to handle governmental requests for access to customer data. Irrespective of the source of the request or the laws that apply, AWS reviews every governmental request individually and independently in accordance with its law enforcement guidelines and commitments in the [AWS Supplementary Addendum](#). AWS rigorously limits – or rejects outright – law enforcement requests for customer data coming from any country, including the US, where they are overly broad or AWS has other appropriate grounds to do so.

Information Request Reports

AWS knows that transparency matters to its customers, AWS regularly publishes an [Amazon Information Request report](#) (IRR) about the types and volume of governmental requests it receives. Beginning with the July-December 2020 report, AWS launched a new IRR format as an organizational supplementary measure that provides more information about the types of governmental requests AWS receives, and the country of origin of such requests. The information provided in the IRRs demonstrates that disclosures by AWS of customer data in response to governmental requests for information are very rare.

Specifically, with respect to requests from US authorities, customers should consider the following FAQ in the IRR (current for the July 2025 report, covering January – June 2025):

“How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?”

None.”

Contractual supplementary measures

Supplementary addendum

The [AWS Supplementary Addendum](#) is part of every customer’s terms and conditions with AWS and sets out supplementary contractual measures to protect customer data. In the [AWS Supplementary Addendum](#), AWS commits to (i) use every reasonable effort to redirect any governmental body requesting customer data to the applicable customer, (ii) promptly notify the applicable customer about the request if legally permitted to do so, and (iii) challenge any

overbroad or inappropriate request, including where the request conflicts with EU law. AWS also commits that if, after exhausting the preceding steps, it remains compelled to disclose customer data, AWS will disclose only the minimum amount of customer data necessary to satisfy the request. To support customers with assessing the laws of recipient countries, AWS warrants that it has no reason to believe that the legislation applicable to AWS or its sub-processors, including in any country to which customer data is transferred, prevents AWS from fulfilling its obligations under the [AWS DPA](#) or the [AWS Supplementary Addendum](#). AWS also commits to promptly notify any change in legislation that is likely to have a substantial impact on AWS fulfilling its obligations.

STEP 5: PROCEDURAL STEPS IF YOU HAVE IDENTIFIED EFFECTIVE SUPPLEMENTARY MEASURES

As step 5 of its DTA, the customer might need to take procedural steps to implement additional supplementary measures depending on the requirements identified in step 4 of its DTA. However, there is no need for a customer to request authorization or pre-approval of such supplementary measures from its competent supervisory authority if the identified supplementary measures do not contradict, directly or indirectly, the SCCs and are sufficient to ensure that the third-country's laws and practices do not undermine the level of protection guaranteed by the GDPR.

STEP 6: RE-EVALUATE AT APPROPRIATE INTERVALS

As step 6 of its DTA, a customer must monitor, on an ongoing basis, developments in the third country to which its customer data will be transferred that could affect the result of its DTA.

- It is the customer's responsibility to constantly evaluate the sufficiency of supplementary measures in order to ensure compliance with the GDPR, the SCCs, and the requirements stipulated by the EDPB.
- AWS will monitor, on an ongoing basis, developments relevant to the transfer of customer data that could affect the basic information provided in this DTA Customer Guide and the level of protection for customer data.

Additional resources

To help customers further understand how they can address their data protection requirements, customers are encouraged to read the risk, compliance and security whitepapers, best practices, checklists and guidance published on the AWS website. This material can be found at <http://aws.amazon.com/compliance> and <http://aws.amazon.com/security>.