Using AWS in the Context of Common Privacy and Data Protection Considerations

First Published September 2016

Updated September 28, 2021

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.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Abstract

This document provides information to assist customers who want to use Amazon Web Services (AWS) to store or process content containing personal data, in the context of common privacy and data protection considerations. It helps customers understand:

- The way AWS services operate, including how customers can address security and encrypt their content.
- The geographic locations where customers can choose to store content and other relevant considerations.
- The respective roles the customer and AWS each play in managing and securing content stored on AWS.

Introduction

This whitepaper focuses on typical questions asked by AWS customers when they are considering privacy and data protection requirements relevant to their use of AWS services to store or process content containing personal data. There are other relevant considerations for each customer to address; for example, a customer may need to comply with industry-specific requirements, the laws of other jurisdictions where that customer conducts business, or contractual commitments a customer makes to a third-party.

This whitepaper is provided solely for informational purposes. It is not legal advice, and should not be relied on as legal advice. As each customer's requirements differ, AWS strongly encourages its customers to obtain appropriate advice on their implementation of privacy and data protection requirements, and on applicable laws and other requirements relevant to their business.

The term "content" in this whitepaper refers to software (including virtual machine images), data, text, audio, video, images, and other content that a customer, or any end user, stores or processes using AWS. For example, a customer's content includes objects that the customer stores using Amazon Simple Storage Service (Amazon S3), files stored on an Amazon Elastic Block Store (Amazon EBS) volume, or the contents of an Amazon DynamoDB database table.

Such content may, but will not necessarily, include personal data relating to that customer, its end users, or third parties. The terms of the AWS Customer Agreement, or any other relevant agreement with AWS governing the use of AWS services, apply to customer content. Customer content does not include data that a customer provides to AWS in connection with the creation or administration of its AWS accounts, such as a customer's names, phone numbers, email addresses, and billing information. AWS refers to this as *account information*, and it is governed by the AWS Privacy Notice. AWS changes constantly, and the AWS Privacy Notice may also change. Check the website frequently to see recent changes.

Considerations relevant to privacy and data protection

Storage of content presents all organizations with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?
- Who will have access to content?
- What laws and regulations apply to the content and what is needed to comply with these?

These considerations are not new and are not cloud-specific. They are relevant to internally hosted and operated systems as well as traditional third-party hosted services. Each may involve storage of content on third-party equipment or on third-party premises, with that content managed, accessed or used by third-party personnel. When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

- What content they choose to store or process using AWS services
- Which AWS services they use with their content
- The Region(s) where their content is stored
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted
- Who has access to their AWS accounts and content and how those access rights are granted, managed and revoked

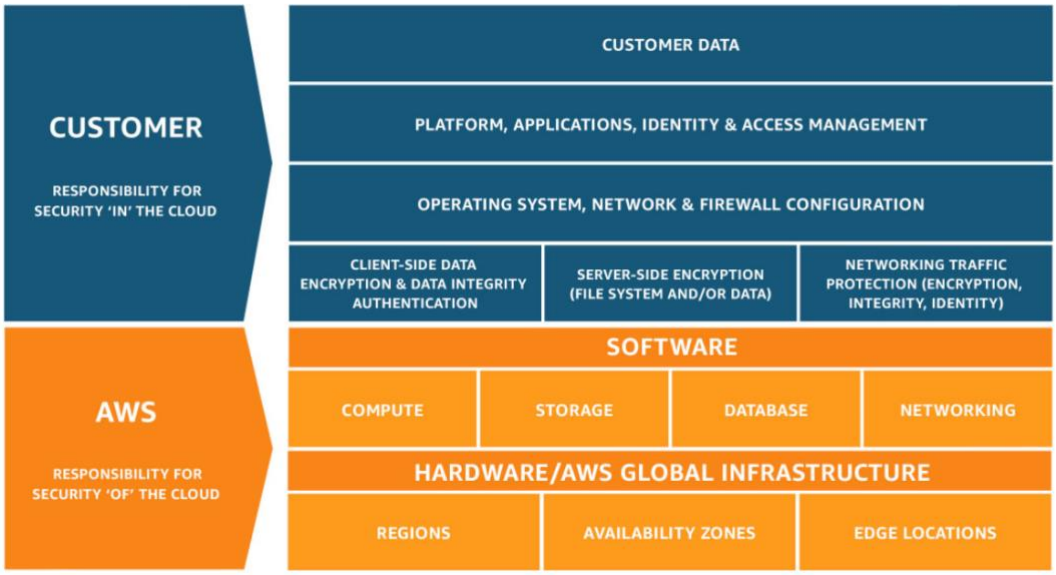
Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS “shared responsibility” model. This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of privacy and data protection requirements that may apply to content that customers choose to store or process using AWS services.

The AWS Shared Responsibility approach to managing cloud security

Will customer content be secure?

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have important roles in the operation and management of security. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security-related features.

The customer generally connects to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections; they are part of the customer's area of responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. The respective roles of the customer and AWS in the shared responsibility model are shown in the following figure:



The AWS Shared Responsibility Model

What does the shared responsibility model mean for the security of customer content?

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:

- Security measures that the cloud service provider (AWS) implements and operates – "security **of** the cloud"
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – "security **in** the cloud".

While AWS manages security **of** the cloud, security **in** the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, applications, systems, and networks – no differently than they would for applications in an onsite data center.

Understanding security OF the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS Cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available, designed to provide optimum availability while providing complete customer segregation. It provides extremely scalable, highly reliable services that enable customers to deploy applications and content quickly and securely, at massive global scale if necessary.

AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical Region in which they store their content. The AWS world-class, highly secure data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24 hours a day, seven days a week by trained security guards, and access is authorized strictly on a least privileged basis. For a complete list of all the security measures built into the core AWS Cloud infrastructure, and services, see the Introduction to AWS Security whitepaper.

AWS is vigilant about its customers' security, and has implemented sophisticated technical and physical measures against unauthorized access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System and Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017, 27018 and 9001 certifications, and PCI DSS Attestation of Compliance.

The AWS ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content. These reports and certifications are produced by independent third-party auditors, and attest to the design and operating effectiveness of AWS security controls.

AWS compliance certifications and reports can be requested at AWS Artifact. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found on the AWS Compliance site.

Understanding security IN the cloud

Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to store or process using AWS services, only the customer can determine what level of security is appropriate for the content they store and process using AWS. Customers also have complete control over which services they use, and whom they empower to access their content and services, including what credentials are required.

Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture.

AWS enables and empowers the customer to decide when and how security measures are implemented in the cloud, in accordance with each customer's business needs. For example, if a higher availability architecture is required to protect customer content, the customer may add redundant systems, backups, locations, network uplinks, and so on to create a more resilient, high availability architecture. If restricted access to customer content is required, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.

To assist customers in designing, implementing, and operating their own secure AWS environment, AWS provides a wide selection of security tools and features customers can use. Customers can also use their own security tools and controls, including a wide variety of third-party security solutions.

Customers can configure their AWS services to leverage a range of such security features, tools and controls to protect their content, including sophisticated identity and access management tools, security capabilities, encryption and network security. Examples of steps customers can take to help secure their content include implementing:

- Strong password policies, assigning appropriate permissions to users, and taking robust steps to protect their access keys.
- Appropriate firewalls and network segmentation, encrypting content, and properly architecting systems to decrease the risk of data loss and unauthorized access.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices, and for security of the content they store or process using AWS services or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, databases, or other services.

AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service (AWS KMS) and AWS CloudTrail.

To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and run security assessments of their organization's use of AWS services, AWS publishes a number of whitepapers relating to security, governance, risk and compliance; and a number of checklists and best practices.

Customers are also free to design and run security assessments according to their own preferences, and can request permission to conduct scans of their cloud infrastructure as long as those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy.

For more information on penetration testing, see the Penetration Testing page.

AWS Regions: Where will content be stored?

AWS data centers are built in clusters in various Regions. Each of these data center clusters in a given country is referred to an "AWS Region". Customers have access to a number of AWS Regions around the world. Customers can choose to use one Region, all Regions, or any combination of AWS Regions. The following figure shows AWS

Region locations as of August 2021. For the most current information on AWS Regions, see the Global Infrastructure page.

AWS Regions

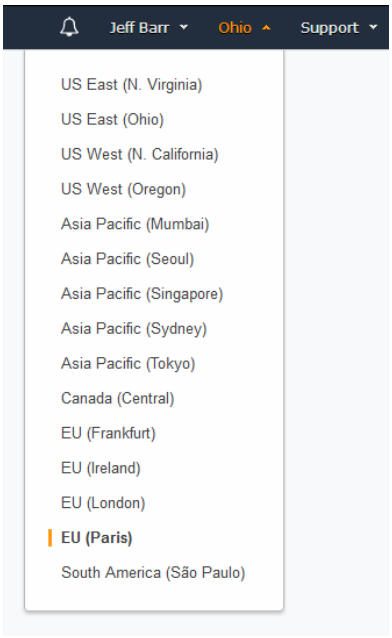
AWS customers choose the AWS Region or Regions in which their content and servers are located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in India can choose to deploy their AWS services exclusively in one AWS Region such as the Asia Pacific (Mumbai) Region and store their content onshore in India, if this is their preferred location. If the customer makes this choice, AWS will not move their content from India without the customer's consent, except as legally required.

Customers always retain control of which AWS Region(s) are used to store and process content. AWS stores and processes each customers' content only in the AWS Region(s) chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required.

How can customers select their Region(s)?

When using the AWS Management Console, or in placing a request through an AWS Application Programming Interface (API), the customer identifies the particular AWS Region(s) where it wants to use AWS services.

The following figure provides an example of the AWS Region selection menu presented to customers when uploading content to an AWS storage service or provisioning compute resources using the AWS Management Console.



Selecting AWS Regions in the AWS Management Console

Customers can also prescribe the AWS Region to be used for their compute resources by taking advantage of the Amazon Virtual Private Cloud (VPC) capability. Amazon VPC lets the customer provision a private, isolated section of the AWS Cloud where the customer can launch AWS resources in a virtual network that the customer defines. With Amazon VPC, customers can define a virtual network topology that closely resembles a traditional network that might operate in their own data center.

Any compute and other resources launched by the customer into the VPC is located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Mumbai) Region and providing a link (either a VPN or Direct Connect) back to the customer's data center, all compute resources launched into that VPC would only reside in the Asia Pacific (Mumbai) Region. This option can also be leveraged for other AWS Regions.

Transfer of personal data cross border

In 2016, the European Commission approved and adopted the new General Data Protection Regulation (GDPR). The GDPR replaced the EU Data Protection Directive, as well as all local laws relating to it. All AWS services comply with the GDPR. AWS

provides customers with services and resources to help them comply with GDPR requirements that may apply to their operations. These include AWS adherence to the CISPE code of conduct, granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards and AWS C5 attestations. For additional information, see the AWS General Data Protection Regulation (GDPR) Center and the Navigating GDPR Compliance on AWS whitepaper.

When using AWS services, customers may choose to transfer content containing personal data cross border, and they need to consider the legal requirements that apply to such transfers. AWS provides a Data Processing Addendum that includes the Standard Contractual Clauses 2010/87/EU (often referred to as "Model Clauses") to AWS customers transferring content containing personal data (as defined in the GDPR) from the EU to a country outside of the European Economic Area.

With the AWS EU Data Processing Addendum and Model Clauses, AWS customers—whether established in Europe or a global company operating in the European Economic Area—can continue to run their global operations using AWS in full compliance with the GDPR. The AWS Data Processing Addendum is incorporated in the AWS Service Terms and applies automatically to the extent the GDPR applies to the customer's processing of personal data on AWS.

Who can access customer content?

Customer control over content

Customers using AWS maintain and do not release effective control over their content within the AWS environment. They can:

- Determine where their content will be located; for example, the type of storage they use on AWS and the geographic location (by AWS Region) of that storage.
- Control the format, structure and security of their content, including whether it is masked, anonymized or encrypted. AWS offers customers options to implement strong encryption for their customer content in transit or at rest, and also provides customers with the option to manage their own encryption keys or use third-party encryption mechanisms of their choice.
- Manage other access controls, such as identity access management, permissions, and security credentials.

This allows AWS customers to control the entire lifecycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention, and deletion.

AWS access to customer content

AWS makes available to each customer the compute, storage, database, networking, or other services, as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features (such as AWS KMS), managing their own encryption keys, or using a third-party encryption mechanism of their own choice. AWS does not access or use customer content without the customer's consent, except as legally required. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Government rights of access

Queries are often raised about the rights of domestic and foreign government agencies to access content held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice from their advisors to understand the application of relevant laws to their business and operations.

AWS policy on granting government access

AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders.

Additionally, AWS notifies customers where practicable before disclosing their content so customers can seek protection from disclosure, unless AWS is legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the Amazon Information Requests Portal online.

Common privacy and data protection considerations

Many countries have laws designed to protect the privacy of personal data. Some countries have one comprehensive data protection law, while others address data protection in a more nuanced way, through a variety of laws and regulations. While legal and regulatory requirements differ — including due to jurisdictional requirements, industry-specific requirements and content-specific requirements — there are some common considerations that arise under several leading data protection laws. These can be aligned to the typical lifecycle of personal data.

To help customers analyze and address their privacy and data protection requirements when using AWS to store and process content containing personal data, this whitepaper discusses various stages of this data lifecycle, identify key considerations relevant to each stage, and provide relevant information about how the AWS services operate.

Many data protection laws allocate responsibilities regarding how a party interacts with personal data, and the level of access and control they have over that personal data. One common approach is to distinguish between a data controller, data processor, and data subject. The terminology used in different jurisdictions may vary, and some laws make more subtle distinctions.

AWS appreciates that its services are used in many different contexts for different business purposes, and that there may be multiple parties involved in the data lifecycle of personal data included in customer content stored or processed using AWS. For simplicity, the guidance in the following table assumes that, in the context of customer content stored or processed using AWS, the customer:

- Collects personal data from its end users or other individuals (data subjects), and determines the purpose for which the customer requires and will use the personal data.
- Has the capacity to control who can access, update, and use the personal data.
- Manages the relationship with the individual about whom the personal data relates (referred to in this section as a data subject), including by communicating with the data subject as required to comply with any relevant disclosure and consent requirements.

As such, the customer performs a role similar to that of a data controller, as it controls its content and makes decisions about treatment of that content, including who is

authorized to process that content on its behalf. By comparison, AWS performs a role similar to that of a data processor, because AWS uses customer content only to provide the AWS services selected by each customer to that customer, and does not use customer content for other purposes without the customer's consent.

> Note that the terms "data processor" and "data controller" have a very distinct meaning under EU law, and this whitepaper is not intended to address specific EU requirements.

Where a customer processes personal data using the AWS services on behalf of and according to the directions of a third-party (who may be the controller of the personal data or another third-party with whom it has a business relationship), the customer responsibilities referenced in the following table will be shared and managed between the customer and that third party.

Table 1 —Data lifecycle stage summary, examples, and considerations

Data lifecycle stage	Summary and examples	Considerations
Collecting personal data	It may be appropriate or necessary to inform individuals (data subjects) or seek their consent before collecting their personal data. This may include notification about the purpose for which their information will be collected, used or disclosed.	**Customer**: The customer determines and controls when, how, and why it collects personal data from individuals, and decides whether it will include that personal data in customer content it stores or processes using the AWS services. The customer may need to disclose the purposes for which it collects that data to the relevant data subjects, obtain the data from a permitted source, and use the data only for a permitted purpose. As between the customer and AWS, the customer has a relationship with the individuals whose personal data the customer stores on AWS, and therefore the customer is able to communicate directly with AWS about collection and treatment of their personal data.

Data lifecycle stage	Summary and examples	Considerations
	Requirements may differ depending on who personal data is collected from (for example, the requirements may differ if personal data is collected from a third-party source instead of directly from the individual). Collection of personal data may only be permitted if it is for a valid or reasonable purpose.	The customer rather than AWS also knows the scope of any notifications given to, or consents obtained by the customer from, such individuals relating to the collection of their personal data. **AWS**: AWS does not collect personal data from individuals whose personal data is included in content a customer stores or processes using AWS, and AWS has no contact with those individuals. Therefore, AWS is unable in these circumstances to communicate with the relevant individuals. AWS uses customer content only to provide the AWS services selected by each customer to that customer, and does not use customer content for any other purposes without the customer's consent.
Using and disclosing personal data	It may be appropriate or necessary to use or disclose personal data only for the purpose for which it was collected.	**Customer**: The customer determines and controls why it collects personal data, what it will be used for, who it can be used by, and who it is disclosed to. The customer must ensure it only does so for permitted purposes. The customer will know whether it uses the AWS services to store or process customer content containing personal data, and therefore is best placed to inform individuals that it will use AWS as a service provider, if required. **AWS**: AWS uses customer content only to provide the AWS services selected by each customer to that customer, and does not use customer content for other purposes without the customer's consent.

Data lifecycle stage	Summary and examples	Considerations
Offshoring personal data	If transferring personal data offshore, it may be necessary or appropriate to inform individuals (data subjects) of the countries in which the customer will store their personal data, and/or seek consent to store their personal data in that location. It may also be important to consider the comparable protections afforded by the privacy regime in the relevant country where personal data will reside.	**Customer**: The customer can choose the AWS Region or Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single Region if preferred. The customer should consider whether it should disclose to individuals the locations in which it stores or processes their personal data and obtain any required consents relating to such locations from the relevant individuals if necessary. As between the customer and AWS, the customer has a relationship with the individuals whose personal data the customer stores on AWS, and therefore the customer is able to communicate directly with them about such matters. **AWS**: AWS stores and processes each customers' content only in the AWS Region(s), and using the services, chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required. If a customer chooses to store content in more than one Region, or copy or move content between Regions, that is solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed. **General**: AWS is ISO 27001 certified and offers robust security features to all customers, regardless of the geographical Region in which they store their content.
Securing personal data	It is important to take steps to protect the security of personal data.	**Customer**: Customers are responsible for security *in* the cloud, including security of their content (and personal data included in their content).

Data lifecycle stage	Summary and examples	Considerations
		Examples of steps customers can take to help secure their content include implementing strong password policies, assigning appropriate permissions to users and taking robust steps to protect their access keys, as well as appropriate firewalls and network segmentation, encrypting content, and properly architecting systems to decrease the risk of data loss and unauthorized access. **AWS**: AWS is responsible for managing the security *of* the underlying cloud environment. For a complete list of all the security measures built into the core AWS Cloud infrastructure, and services, see the Introduction to AWS Security whitepaper. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System and Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017, and 27018 certifications, and PCI DSS Attestation of Compliance.
Accessing and correcting personal data	Individuals (data subjects) may have right to access their personal data, including for the purposes of correcting it.	**Customer**: The customer retains control of content stored or processed using AWS, including control over how that content is secured and who can access and amend that content. In addition, as between the customer and AWS, the customer has a relationship with the individuals whose personal data is included in customer content stored or processed using AWS services. The customer rather than AWS is therefore able to work with relevant individuals to provide them access to, and the ability to correct, personal data included in customer content.

Data lifecycle stage	Summary and examples	Considerations
		AWS: AWS only uses customer content to provide the AWS services selected by each customer to that customer or as otherwise consented to by the customer. AWS does not have a direct relationship with the individuals whose personal data is included in content a customer stores or processes using the AWS services. Given this, and the level of control customers enjoy over customer content, AWS does not provide individuals with access to, or the ability to correct, their personal data.
Maintaining the quality of personal data	It may be important to ensure that personal data is accurate, and that integrity of that personal data is maintained.	**Customer**: When a customer chooses to store or process content containing personal data using AWS, the customer has control over the quality of that content and the customer retains access to and can correct it. This means that the customer can keep the personal data included in customer content accurate, complete, not misleading, and up-to-date. **AWS**: The AWS SOC 1, Type 2 report includes controls that provide reasonable assurance that data integrity is maintained through all phases including transmission, storage, and processing.
Deleting or de-identifying personal data	Personal data typically should not be kept for longer than is reasonably required, and otherwise should be retained in accordance with relevant data retention laws.	**Customer**: Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymize the personal data when no longer needed. **AWS**: The AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation.

Privacy breaches

Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators, and affected individuals as required under applicable law. Only the customer can manage this responsibility.

For example, customers control access keys, and determine who is authorized to access their AWS account. AWS does not have visibility of access keys, or who is and who is not authorized to log into an account. Therefore, the customer is responsible for monitoring use, misuse, distribution, or loss of access keys.

In some jurisdictions it is mandatory to notify individuals or a regulator of unauthorized access to or disclosure of their personal data. There are circumstances in which notifying individuals will be the best approach to mitigate risk, even though it is not mandatory under the applicable law. The customer determines when it is appropriate or necessary for them to notify individuals, and the notification process they will follow.

Considerations

Customers should consider the specific requirements that apply to them, including any industry-specific requirements. The relevant privacy and data protection laws and regulations applicable to individual customers depend on several factors, including where a customer conducts business, the industry in which they operate, the type of content they want to store, where or from whom the content originates, and where the content will be stored.

Customers concerned about their privacy regulatory obligations should first ensure they identify and understand the requirements that apply to them, and seek appropriate advice.

Conclusion

For AWS, security is always top priority. AWS delivers services to millions of active customers, including enterprises, educational institutions, and government agencies in over 190 countries. AWS customers include financial services providers and healthcare providers, and AWS is trusted with some of their most sensitive information.

AWS services are designed to give customers flexibility over how they configure and deploy their solutions and how they control their content, including where it is stored, how it is stored, and who has access to it. AWS customers can build their own secure applications and store content securely on AWS.

Contributors

Contributors to this document include:

- Simon Hollander, AWS Legal, Senior Corporate Counsel
- Jonathan Hatae, AWS Legal, Senior Corporate Counsel

Further reading

To help customers further understand how they can address their privacy and 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
- http://aws.amazon.com/security

As of the date of this writing, specific whitepapers about privacy and data protection considerations are also available for the following countries or Regions:

- California
- European Union
- Germany
- Australia
- Hong Kong
- Japan
- Malaysia
- New Zealand
- Philippines

- Singapore

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS Cloud, and gain proficiency with AWS services and solutions. AWS offers free instructional videos, self-paced labs, and instructor-led classes.

Further information on AWS training is available at: http://aws.amazon.com/training/.

AWS certifications certify the technical skills and knowledge associated with the best practices for building secure and reliable cloud-based applications using AWS technology.

Further information on AWS certifications is available at: http://aws.amazon.com/certification/.

If you require further information, contact AWS at: https://aws.amazon.com/contact-us/ or contact your local AWS account representative.

Document revisions

Date	Description
September 28, 2021	Refreshed to reflect latest information about AWS services and infrastructure
May 2018	Fourth Publication
February 2018	Third Publication
December 2016	Second Publication
September 2016	First Publication