Using AWS in the Context of Thai Privacy Considerations

April 14, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this whitepaper. This whitepaper: (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 whitepaper is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This whitepaper provides information to assist customers who want to use Amazon Web Services (AWS) services to store or process content that contains personal data, in the context of key privacy and data protection considerations and the Personal Data Protection Act, B.E. 2562 (2019) Personal data (PDPA). It helps customers understand the following:

- The way AWS services operate, including how customers can address security and encrypt their customer content
- 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 the implications of the PDPA on their use of AWS services to store or process content that contains personal data. Beyond the PDPA, there may be 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. These considerations fall outside the scope of this whitepaper.

This whitepaper is provided solely for informational purposes. It is not legal advice and should not be relied on as legal advice. Because 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 that are relevant to their business.

The terms "content" or "customer content" in this whitepaper refer to software (including virtual machine images), data, text, audio, video, or images that a customer, or any end user, transfers to AWS for processing, storage, or hosting by AWS services in connection with a customer's account, and any computational results that a customer or their end user derives from the foregoing through their use of AWS services. For example, customer content includes content that the customer, or any end user, stores by using Amazon Simple Storage Service (Amazon S3).

Such content may, but will not necessarily, include personal data that relates to that customer, its end users, or third parties. The terms of the AWS Customer Agreement and the Service Terms, 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 AWS uses account information in accordance with the AWS Privacy Notice. The AWS Privacy Notice may be updated from time to time. Check the AWS site 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 customer maintains ownership and control of their customer content, including control over:

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

Because customers retain ownership and control over their customer 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 by using AWS services.

The AWS Shared Responsibility Model for managing cloud security

Security and compliance are shared responsibilities between AWS and the customer. This section discusses the AWS Shared Responsibility Model and addresses some common questions.

Will customer content be secure?

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, meaning that 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 Figure 1.

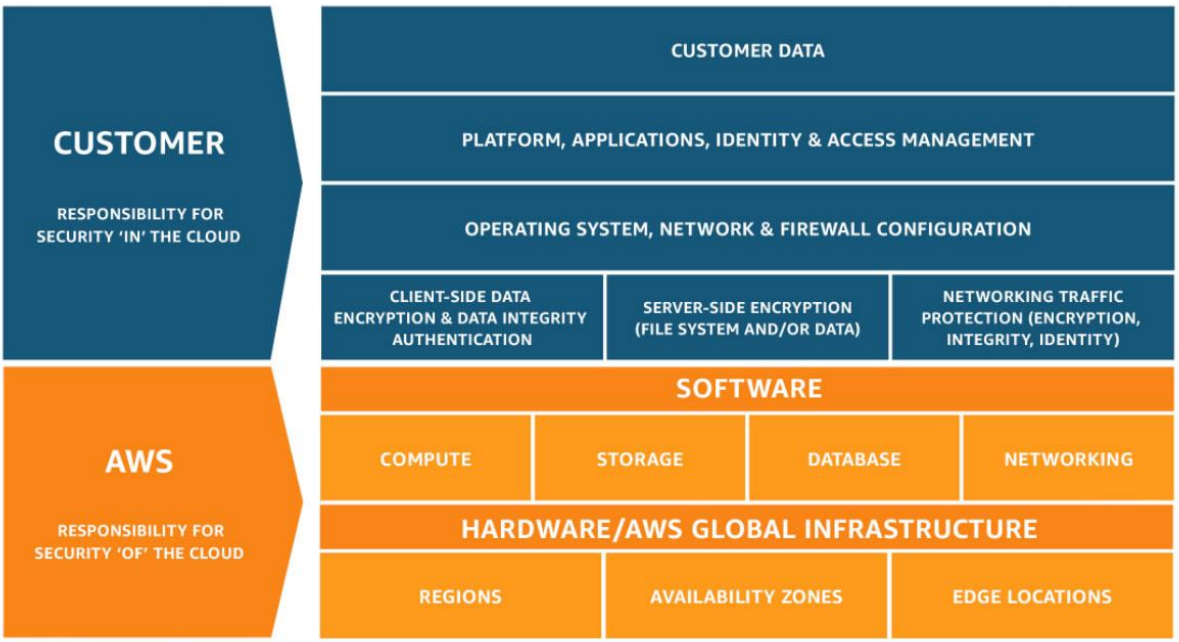

Figure 1 – The AWS Shared Responsibility Model

What does the AWS 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 these concepts:

- 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"

Although AWS manages security **of** the cloud, security **in** the cloud is the responsibility of the customer, because customers retain control of what security they choose to implement to protect their own customer 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 separation between environments. 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 geographic location (by AWS Region) in which they store their customer content. AWS operates world-class, highly secure data centers that use 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 AWS 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 Controls (SOC) 1, 2 and 3 reports, ISO/IEC 27001, 27017, 27018 and ISO 9001 certifications, and PCI DSS Attestation of Compliance.

The AWS ISO/IEC 27018 certification demonstrates that AWS has a system of controls in place that specifically addresses 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. You can request AWS compliance certifications and reports 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 customer content when they use AWS services. Customers, not 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 services. Customers have complete control over which AWS services they use and whom they empower to access their customer content and services, including what credentials are required.

Customers control how they configure their environments and secure their customer content, including whether they encrypt their customer 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, because these settings are determined and controlled by the customer. 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, geographic 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 that 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 use a range of such security features, tools, and controls to protect their customer content, including sophisticated identity and access management tools, security capabilities, encryption, and network security. Examples of steps customers can take to help secure their customer content include the following:

- Implementing strong password policies, enabling multi-factor authentication (MFA), assigning appropriate permissions to users, and taking robust steps to protect their access keys.

- Setting up 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 customer content effectively, including AWS Key Management Service (AMS KMS) and AWS CloudTrail.

To assist customers in integrating AWS security controls into their existing control frameworks and help customers to 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.

Subject to AWS policies regarding testing (see Penetration Testing), 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 AWS Penetration Testing page.

AWS Regions: Where will content be stored?

AWS data centers are built in clusters in various global AWS Regions. Each of these data center clusters in a given country is referred to in this whitepaper as an *AWS Region* or *Region*. Customers have access to a number of AWS Regions around the world. Customers can choose to use one AWS Region, all AWS Regions, or any combination of AWS Regions. Figure 2 shows AWS Region locations as of April 2023. For the most current information on AWS Regions, see Global Infrastructure.

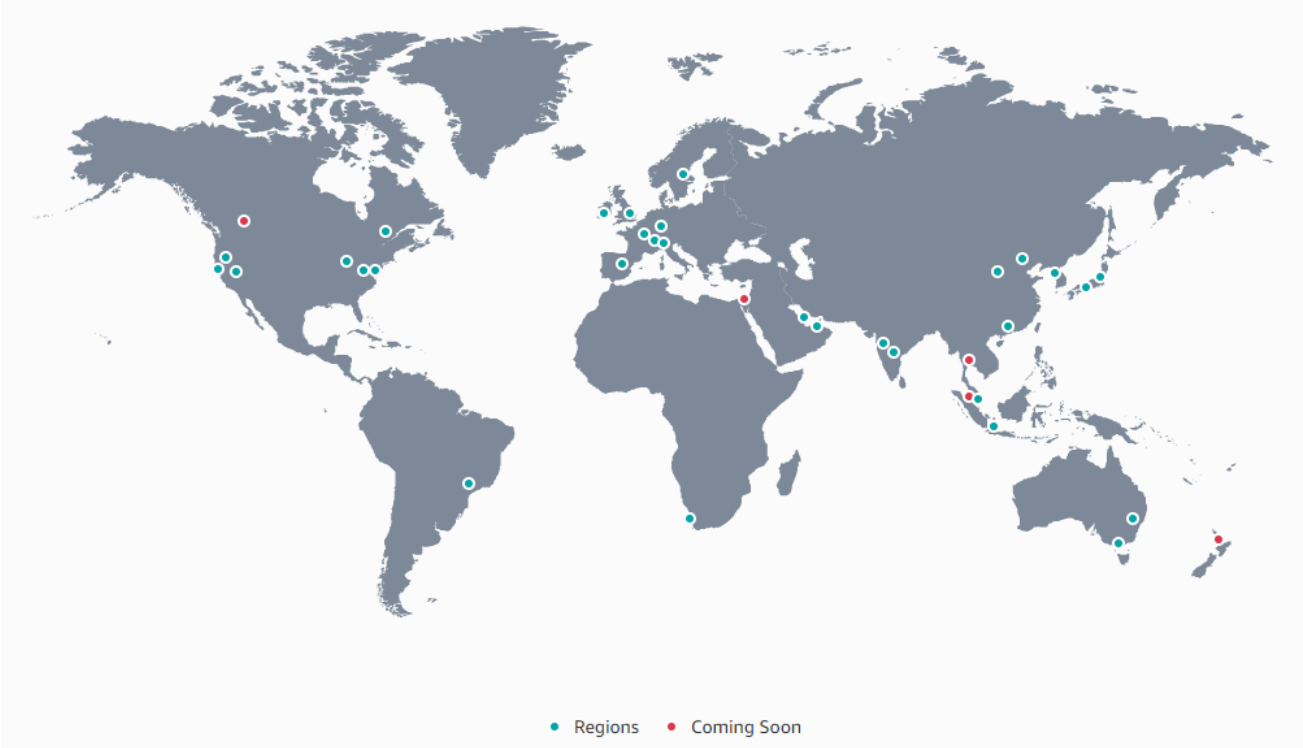

Figure 2 – AWS Regions

Customers choose the AWS Region or Regions in which their customer content and servers are located. This allows customers with geographic specific requirements to establish environments in a single geographic location or in multiple geographic locations of their choice. For example, customers in Thailand can choose to deploy their AWS services exclusively in one AWS Region, such as the Asia Pacific (Singapore) Region, and store their customer content onshore in Singapore, if this is their preferred geographic location.

Customers can use AWS services with the confidence that their customer content stays in the AWS Region that they select. AWS stores and processes each customer's content only in the AWS Region or Regions chosen by the customer, and otherwise will not move customer content without the customer's consent, except as agreed with customers. A small number of AWS services involve the transfer of customer content. For example, content might be moved to develop and improve those services, where customers can opt out of the transfer, or because transfer is an essential part of the service (such as a content

delivery service).

How can customers select their Region?

When a customer uses the AWS Management Console, or places a request through an AWS API, the customer identifies the particular AWS Region or Regions where they want to use AWS services.

Figure 3 provides an example of the AWS Region selection menu that is presented to customers when they upload content to an AWS storage service or provision compute resources by using the AWS Management Console.

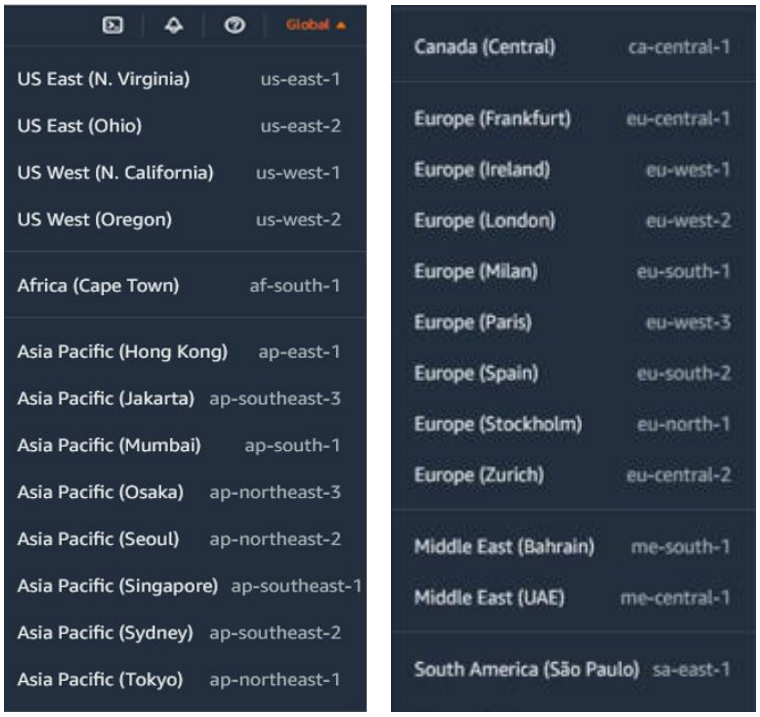

Figure 3 - Selecting AWS Regions in the AWS Management Console

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 are located in the AWS Region designated by the customer. For example, when you create a VPC in the Asia Pacific (Singapore) Region and provide a link (either a VPN or AWS Direct Connect connection) back to the customer's data center, this causes all compute resources launched into that VPC to only reside in the Asia Pacific (Singapore) Region.

Transfer of personal data cross-border

Customers can use AWS services to process personal data that has been uploaded to the AWS services under their AWS accounts, and AWS is committed to offering services and resources to customers to help them comply with their legal requirements that may apply to their activities. These services include access controls, monitoring and logging tools, and encryption services.

When using AWS services, customers may choose to transfer content that contains personal data across borders, and they need to consider the legal requirements that apply to such transfers. AWS provides a Data Processing Addendum (AWS DPA) that helps customers to comply with contractual obligations under applicable data protection regulations (e.g., GDPR). The AWS DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require the AWS DPA to comply with applicable data protection law. The Service Terms also include the Standard Contractual Clauses adopted by the European Commission in June 2021, and the AWS DPA confirms that the Standard Contractual Clauses apply automatically whenever a customer uses AWS services to transfer personal data to countries outside of the European Economic Area that have not received an adequacy decision from the European Commission (third countries).

Who can access customer content?

Customers maintain ownership and control of their customer content and select which AWS services process, store, and host their customer content. This section discusses access to such customer content and addresses common questions.

Customer control over customer content

AWS is vigilant about your privacy, and AWS is architected to be the most flexible and secure cloud computing environment available today. With AWS, customers own their customer content, customers control the geographic location of its storage, and customers control who has access to this content. AWS is transparent about how AWS services process the personal data that customers upload to their AWS account, and AWS provides capabilities that allow customers to encrypt, delete, and monitor the processing of that customer content.

Customers can do the following:

- Determine where their customer 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 customer 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 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 AWS compute, storage, database, networking, or other services, as described on its website. Customers have a number of options to encrypt their customer content when they use AWS 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 prohibits, and AWS systems are designed to prevent, remote access by AWS personnel to customer content for any purpose, including service maintenance, unless access is requested by the customer, is required to prevent fraud or abuse, or to comply with law.

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 customer content. The local laws that apply in the jurisdiction where customer 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

If AWS receives a legal request for customer content, it will not disclose customer content unless required to do so to comply with a legally valid and binding order of a governmental body or as otherwise required by applicable law.

If compelled to disclose customer content to a governmental body, AWS will give customers reasonable notice of the demand, to allow the customer to seek a protective order or other appropriate remedy, 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 Law Enforcement Information Requests Portal.

Privacy and data protection in Thailand: the PDPA

This part of the paper discusses aspects of the PDPA that relate to data protection. The PDPA came into effect on June 1, 2022. The data protection principles under the PDPA impose requirements for collecting, using, disclosing, transferring, and processing personal data.

The PDPA makes a distinction between a *data controller* that makes decisions regarding the collection, use, or disclosure of personal data, and a *data processor* that processes personal data on behalf of a data controller.

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 that is stored or processed by using AWS services. For simplicity, the information included in the following table assumes that, in the context of the customer content stored on the AWS services, the customer does the following:

- Collects personal data from its end users or other individuals 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, including by communication with the individual as required to comply with any relevant notification and consent requirements

Customers may in fact work with or rely on third parties to discharge these responsibilities, but the customer, not AWS, manages its relationships with third parties.

We summarize some data protection principles from the PDPA in the following table. We also discuss aspects of the AWS services that are relevant to these requirements.

Data protection principle	Summary of data protection obligations	Considerations
Consent, collection, notification, and purpose of use	Personal data can be collected and used where: the individual has given valid consent; or there is a lawful basis (for example, contractual obligation or legitimate interest). Data controllers must inform the individuals of the purposes for which their personal data is being collected and processed.	**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 notify individuals or publicly announce the purposes for collecting data and any other information required by the PDPA. The customer should only collect personal data from a permitted source and use personal data for a permitted purpose. As between the customer and AWS, the customer has a relationship with the individuals, and therefore the customer is able to communicate directly with such individuals about collection and treatment of their personal data. The customer, not AWS, also knows the scope of any notifications given to, or consents obtained by the customer from, such individuals relating to the collection, use, and processing 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 the AWS services, and AWS has no contact with those individuals. Therefore, in these circumstances, AWS is unable to communicate with the relevant individuals.

Data protection principle	Summary of data protection obligations	Considerations
Access, correction, and deletion of personal data	Individuals should be able to access, correct, and delete their personal data	**Customer:** The customer retains control of content that is stored or processed using AWS services, including control over how that content is secured and who can access, amend, and delete that content. In addition, as between the customer and AWS, the customer has a relationship with the individuals. The customer, rather than AWS, is therefore able to work with relevant individuals to provide them access to personal data included in customer content, with the ability to delete as well as to correct such personal data. **AWS:** AWS has no contact with the individuals whose personal data is included in content a customer stores or processes using the AWS services. Given this, and the fact that customers retain control of content that is stored or processed using AWS services, AWS is unable to provide such individuals with access to, or the ability to delete or correct, their personal data.
Maintaining the accuracy of personal data	Data controllers must ensure that personal data remains accurate, up to date, complete, and not misleading.	**Customer:** When a customer chooses to store or process personal data using AWS, the customer has control over the quality of that personal data, and the customer retains access to and can correct it. This means that the customer must take all required steps to ensure that the personal data is accurate, complete, not misleading and kept up to date. **AWS**: The AWS System and Organization Controls (SOC) 2 Type II report includes controls that provide

Data protection principle	Summary of data protection obligations	Considerations
		reasonable assurance that data integrity is maintained through all phases, including transmission, storage, and processing. However, as noted above, customers remain responsible for the quality of any personal data stored or processed using AWS services.
Securing personal data	Data controllers must provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, modification, or disclosure of personal data.	**Customer:** Customers are responsible for security **in** the cloud, including security of their content (and personal data included in their content). If the customer chooses to include personal data in customer content stored or processed using AWS services, the customer controls the format and structure of the content and how it is protected from disclosure to unauthorized parties, including whether it is anonymized or encrypted. Examples of steps customers can take to help secure their content include implementing strong password policies, enabling multi-factor authentication (MFA), assigning appropriate permissions to users, and taking robust steps to protect users' 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 list of all the security measures built into the core AWS Cloud infrastructure and services, see the Introduction to AWS Security whitepaper.

Data protection principle	Summary of data protection obligations	Considerations
		Customers can validate the security controls that are in place within the AWS environment through AWS certifications and reports, including the AWS System and Organization Controls (SOC) 1, 2 and 3 reports, ISO 27001, 27017, and 27018 certifications, and the PCI DSS Attestation of Compliance.
International transfer of personal data	Data controllers may only transfer personal data to a foreign country where such country has adequate data protection standards, unless otherwise permitted by the PDPA.	**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. AWS services are structured so that a customer maintains effective control of customer content, regardless of what Region they use for their content. The customer should consider whether it should disclose to individuals the locations in which it stores or processes those individuals' 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, and therefore the customer is able to communicate directly with them about such matters. **AWS:** AWS enables customers to use AWS services with the confidence that their customer data stays in the AWS Region that customers select. If a customer chooses to store content in more than one Region, or copy or move content between Regions, that is

Data protection principle	Summary of data protection obligations	Considerations
		solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed. 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 transfer is an essential part of the service (such as a content delivery service).
Retention and deletion	Personal data should not be kept longer than necessary for the fulfilment of the lawful purpose for which the personal data was collected or retained.	**Customers:** Only the customer knows why personal data included in customer content that is stored or processed using AWS services was collected, and only the customer knows when it is required to retain that personal data for its legal or business purposes. The customer should delete or anonymize the personal data when no longer needed. **AWS**: AWS does not know what type of content the customer chooses to store in AWS, and the customer retains control over how their content is stored, used, and protected from disclosure. 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 customer content when they use AWS services, 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 sign in to an account. Therefore, the customer is responsible for monitoring use, misuse, distribution, or loss of access keys.

In Thailand, the PDPA requires data controllers to notify the regulator in the event of unauthorized access, use, disclosure, modification, or alteration of personal data, if the breach meets a certain level of risk. Where a privacy breach has a high level of risk, data controllers are also required to notify the data subjects of such breach and the remedial actions taken. There are circumstances in which notifying individuals will be the best approach to mitigate risk, even if not mandatory. The customer determines when it is appropriate or necessary for them to notify individuals, and the notification process they will follow.

Consideration

This whitepaper does not discuss specific requirements that may also be relevant to customers, including industry-specific requirements. The relevant privacy and data protection laws and regulations that are 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 wish 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 that 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 more than 190 countries. 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. Customers can build their own secure applications and store content securely on AWS.

Further reading

To 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:

- aws.amazon.com/compliance
- aws.amazon.com/security

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 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 by using AWS technology. Further information on AWS certifications is available at:

- aws.amazon.com/certification/

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

Document Revisions

Date	Description
April 2023	First publication