Using AWS in the Context of Hong Kong Privacy Considerations

May 2018

(Please consult https://aws.amazon.com/compliance/resources/
for the latest version of this paper)

Overview

This document provides information to assist customers who want to use AWS to store or process content containing personal data, in the context of common privacy and data protection considerations and the Hong Kong Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO). It will help 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 services

Scope

This whitepaper focuses on typical questions asked by AWS customers when they are considering implications of the PDPO relevant to their use of AWS services to store or process content containing personal data. There will also 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.

This paper 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 will 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.

When we refer to content in this paper, we mean software (including virtual machine images), data, text, audio, video, images and other content that a customer, or any end user, stores or processes using the AWS services. For example, a customer's content includes objects that the customer stores using Amazon Simple Storage Service, files stored on an Amazon Elastic Block Store 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 us governing the use of AWS services, apply to customer content. Customer content does not include data that a customer provides to us in connection with the creation or administration of its AWS accounts, such as a customer's names, phone numbers, email addresses and billing information - we refer to this as account information and it is governed by the AWS Privacy Policy[1].

[1] http://aws.amazon.com/privacy/

Customer Content: 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.

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 will generally connect to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore 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:

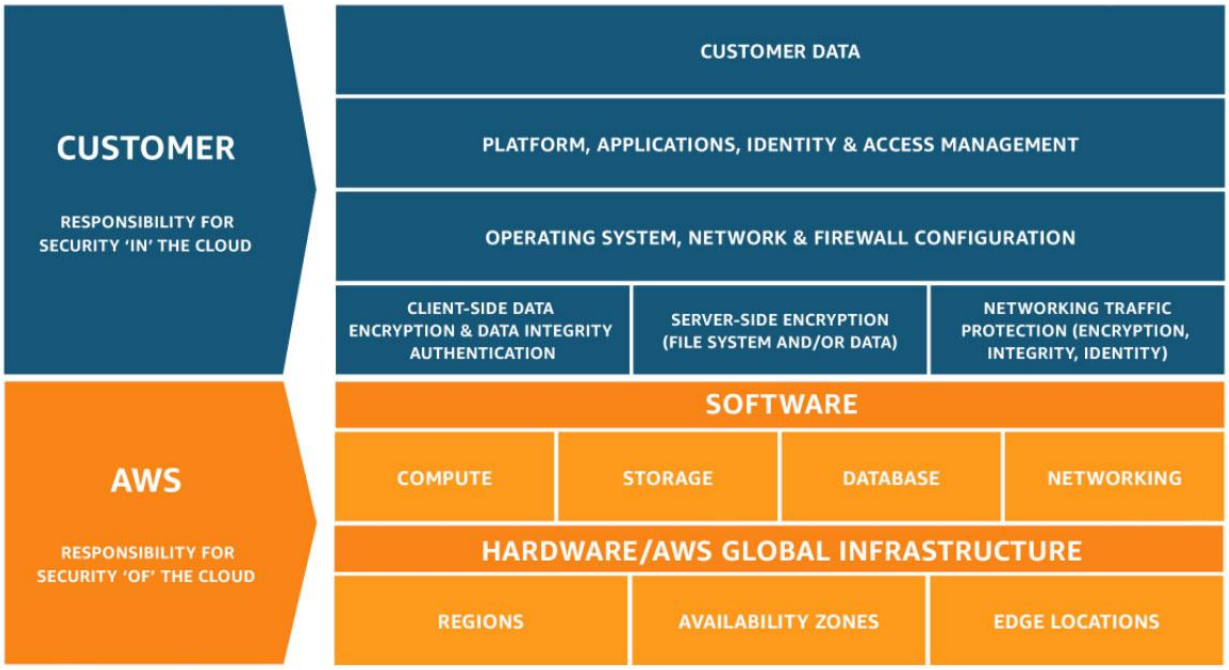


Figure 1 – Shared Responsibility Model

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 on-site 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. AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 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, please read our Overview of Security Processes[2] whitepaper.

We are vigilant about our customers' security and have 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 & Organization Control (SOC) 1, 2[3] and 3[4] reports, ISO 27001[5], 27017[6], 27018[7] and 9001[8] certifications and PCI DSS[9] compliance reports. Our 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

[2] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
[3] https://aws.amazon.com/compliance/soc-faqs/
[4] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[5] http://aws.amazon.com/compliance/iso-27001-faqs/
[6] http://aws.amazon.com/compliance/iso-27017-faqs/
[7] http://aws.amazon.com/compliance/iso-27018-faqs/
[8] https://aws.amazon.com/compliance/iso-9001-faqs/
[9] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found at AWS' compliance site[10].

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 will be 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 will be 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, etc. 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.

[10] https://aws.amazon.com/compliance/

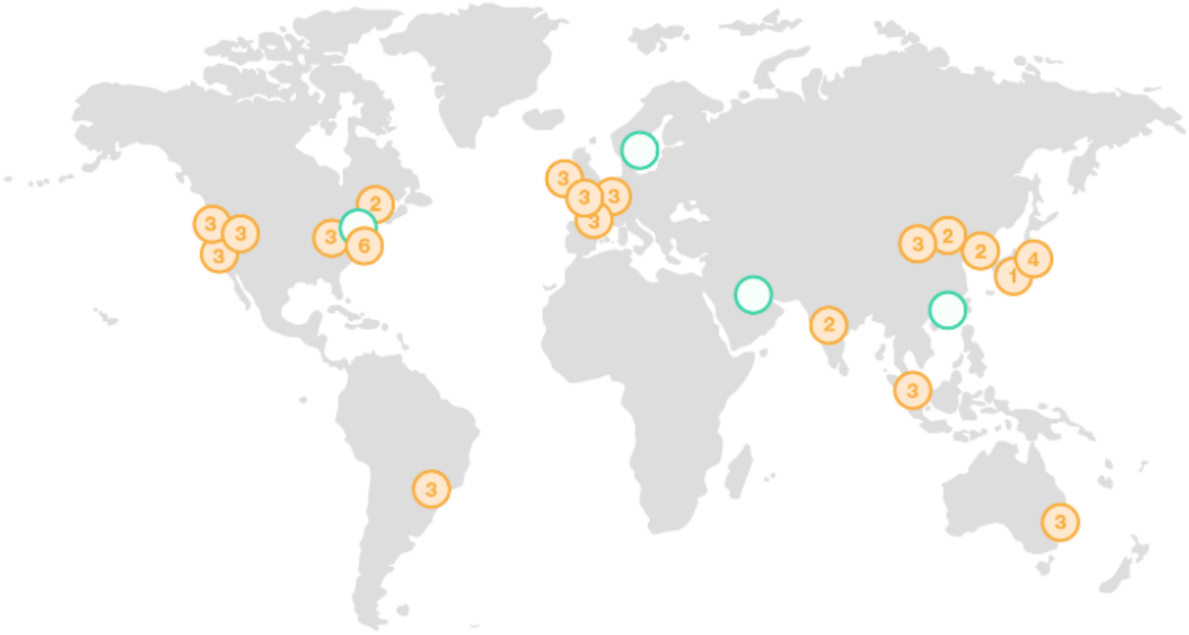
AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service and AWS CloudTrail. To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and execute security assessments of their organization's use of AWS services, AWS publishes a number of whitepapers[11] relating to security, governance, risk and compliance; and a number of checklists and best practices. Customers are also free to design and execute 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[12].

[11] http://aws.amazon.com/compliance/#whitepapers

[12] https://aws.amazon.com/aup/

AWS Regions: Where will content be stored?

AWS data centers are built in clusters in various global regions. We refer to each of our data center clusters in a given country as an "AWS Region". Customers have access to a number of AWS Regions around the world[13]. Customers can choose to use one Region, all Regions or any combination of AWS Regions. Figure 2 shows AWS Region locations as at May 2018.[14]



Region & Number of Availability Zones

US East
N. Virginia (6),
Ohio (3)

US West
N. California (3),
Oregon (3)

Asia Pacific
Mumbai (2),
Seoul (2),
Singapore (3),
Sydney (3),
Tokyo (4),
Osaka-Local (1)[1]

Canada
Central (2)

China
Beijing (2),
Ningxia (3)

Europe
Frankfurt (3),
Ireland (3),
London (3),
Paris (3)

South America
São Paulo (3)

AWS GovCloud (US-West) (3)

New Region (coming soon)

Bahrain

Hong Kong SAR, China

Sweden

AWS GovCloud (US-East)

Figure 2 – AWS Global Regions

[13] AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. AWS China (Beijing) is also an isolated AWS Region. Customers who wish to use the AWS China (Beijing) Region are required to sign up for a separate set of account credentials unique to the China (Beijing) Region.

[14] For a real-time location map, please visit: https://aws.amazon.com/about-aws/global-infrastructure/

AWS customers choose the AWS Region or Regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in Singapore can choose to deploy their AWS services exclusively in one AWS Region such as the Asia Pacific (Singapore) Region and store their content onshore in Singapore, if this is their preferred location. If the customer makes this choice, AWS will not move their content from Singapore 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 only stores and processes each customers' content 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.

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 wishes to use AWS services.

Figure 3: Selecting AWS Global Regions 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.

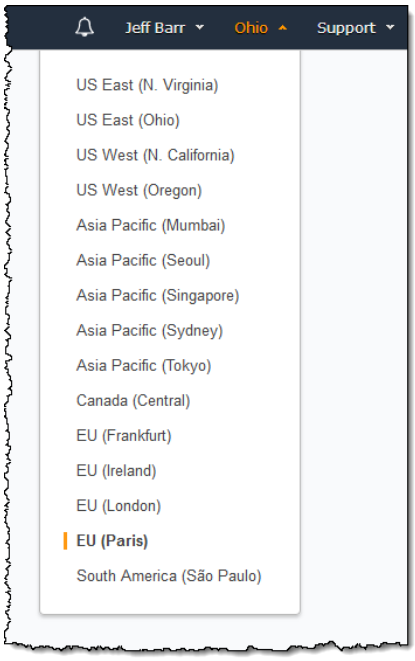


Figure 3 – Selecting AWS Global Regions in the AWS Management Console

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 will be located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Singapore) Region and providing a link (either a VPN[15] or Direct Connect[16]) back to the customer's data center, all compute resources launched into that VPC would only reside in the Asia Pacific (Singapore) 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, please visit the AWS General Data Protection Regulation (GDPR) Center[17] and see our Navigating GDPR Compliance on AWS Whitepaper[18].

When using AWS services, customers may choose to transfer content containing personal data cross border, and they will 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 our 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.

[15] https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html
[16] https://aws.amazon.com/directconnect/
[17] https://aws.amazon.com/compliance/gdpr-center/
[18] https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

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 life-cycle 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 Key Management Service), 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 to understand the application of relevant laws to their business and operations.

When concerns or questions are raised about the rights of domestic or foreign governments to seek access to content stored in the cloud, it is important to understand that relevant government bodies may have rights to issue requests for such content under laws that already apply to the customer. For example, a company doing business in Country X could be subject to a legal request for information even if the content is stored in Country Y. Typically, a government agency seeking access to the data of an entity will address any request for information directly to that entity rather than to the cloud provider.

Most countries have legislation that enables law enforcement and government security bodies to seek access to information. In fact, most countries have processes (including Mutual Legal Assistance Treaties) to enable the transfer of information to other countries in response to appropriate legal requests for information (e.g. relating to criminal acts). However, it is important to remember that each relevant law will contain criteria that must be satisfied in order for the relevant law enforcement body to make a valid request. For example, the government agency seeking access may need to show it has a valid reason for requiring a party to provide access to content, and may need to obtain a court order or warrant.

Many countries have data access laws which purport to apply extraterritorially. An example of a U.S. law with extra-territorial reach that is often mentioned in the context of cloud services is the U.S. Patriot Act. The Patriot Act is similar to laws in other developed nations that enable governments to obtain information with respect to investigations relating to international terrorism and other foreign intelligence issues. Any request for documents under the Patriot Act requires a court order demonstrating that the request complies with the law, including, for example, that the request is related to legitimate investigations. The Patriot Act generally applies to all companies with an operation in the U.S., irrespective of where they are incorporated and/or operating globally and irrespective of whether the information is stored in the cloud, in an on-site data center or in physical records. This means that companies headquartered or operating outside the United States, which also do business in the United States, may find they are subject to the Patriot Act by reason of their own business 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 in order 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, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, please visit the Amazon Information Requests Portal online[19].

[19] https://aws.amazon.com/compliance/amazon-information-requests/

Privacy and Data Protection in Hong Kong: The Personal Data (Privacy) Ordinance

The main requirements for handling personal data are set out in the Data Protection Principles (DPP) of the PDPO. The DPPs impose requirements for collecting, managing, using, disclosing and otherwise handling personal data collected from individuals in Hong Kong.

The PDPO distinguishes between "data users" and "data processors". "Data users" control the collection, holding, processing or use of personal data. "Data processors" process personal data on behalf of others and do not process data for their own purposes.

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 information included in customer content stored or processed using AWS services. For simplicity, the guidance included in the table below assumes that, in the context of the customer content stored on the AWS services, the customer:

- Acquires personal information from their end users, and determines the purpose for which they require and will use the personal information
- Has the capacity to control who can access, update and use the personal information
- Manages the relationship with the individual about whom the personal information relates, including by communication with the individual as required to comply with any relevant disclosure and consent requirements

Customers may in fact work with or rely on third parties to discharge these responsibilities, but the customer, rather than AWS, would manage its relationships with third parties.

We summarize certain DPP requirements that are particularly important for a customer to consider if using AWS to store personal data in the table below. We also discuss aspects of the AWS services relevant to these requirements.

Data Protection Principle	Summary of Data Protection Obligations	Considerations
Purpose and manner of collection of personal data	Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. Data collected should be necessary but not excessive.	**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 must ensure that personal data is collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. 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 collection and treatment of their personal data. The customer rather than AWS will also know 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 not required and is unable in the circumstances to communicate with the relevant individuals. AWS will not know the nature of the customer content used by the customer with the AWS services. AWS only uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for any other purposes.
Accuracy and duration of retention of personal data	Data users must take all practicable steps to ensure that personal data is accurate with regard to the purpose for which the personal data is being, or will be, used. If the data user has reasonable grounds to believe personal data is inaccurate with regard to	**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 must take all required steps to ensure that personal data included in customer content is accurate, complete, not misleading and kept up-to-date.

Data Protection Principle	Summary of Data Protection Obligations	Considerations
	the purpose for which it is being or will be used, the personal data should not be used for that purpose unless either those grounds cease to apply, or the data is erased. Personal data should not be kept for longer than is necessary for the fulfillment of the purpose for which the data is being or will be used.	Only the customer knows why personal data included in customer content stored on AWS was collected, how it will use the personal data, 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 SOC 1, Type 2 report includes controls that provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. The AWS services provide the customer with controls to enable the customer to delete content, as described in AWS Documentation[20].
Use of personal data	Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.	**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. **AWS:** AWS only uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes.
Security of personal data	Data users should take all practicable steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure, loss or use. Where data users engage data processors to process personal data on their behalf, the data user must adopt contractual or other means to prevent unauthorized or	**Customer:** Customers are responsible for their content and for security in the cloud, including security of their content (and personal data included in their content). **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, please read our Overview of Security Processes[21] whitepaper. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System &

[20] https://aws.amazon.com/documentation/

[21] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Data Protection Principle	Summary of Data Protection Obligations	Considerations
	accidental access, processing, erasure, loss or use of the data transferred to the data processor.	Organization Control (SOC) 1, 2[22] and 3[23] reports, ISO 27001[24], 27017[25] and 27018[26] certifications and PCI DSS[27] compliance reports.
Information to be generally available	Data users should take all practicable steps to ensure that the public can ascertain its personal data policies and practices, be informed of the kind of personal data the data user holds and the main purposes for which this data is to be used.	**Customer:** The customer is responsible for maintaining its own privacy policy that complies with the PDPO and ensuring that these matters can be ascertained by the public. **AWS:** AWS does not know when a customer chooses to upload to AWS content that contains personal data, 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. AWS only uses customer content to provide the AWS services selected by each customer to that customer, and does not use customer content for other purposes.
Access to personal data	Data subjects must be given access to their personal data and allowed to make corrections if it is inaccurate.	**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. **AWS:** AWS only uses customer content to provide the AWS services selected by each customer to that customer, and AWS has no contact with the individuals whose personal

[22] http://aws.amazon.com/compliance/soc-faqs/
[23] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[24] http://aws.amazon.com/compliance/iso-27001-faqs/
[25] http://aws.amazon.com/compliance/iso-27017-faqs/
[26] http://aws.amazon.com/compliance/iso-27018-faqs/
[27] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

Data Protection Principle	Summary of Data Protection Obligations	Considerations
		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 is not required, and is unable in the circumstances, to provide such individuals with access to, or the ability to correct, their personal data.
Offshoring personal data	If transferring personal data offshore, it may be 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. The cross border data transfer restriction in Hong Kong (Section 33 of the PDPO) was passed into law in 1995 at the time the PDPO was first introduced. However, as at December 2017 the section has not been brought into operation.	**Customer:** The customer can choose the AWS Region or Regions in which to align to their requirements, and 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 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 only stores and processes each customers' content 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. AWS is ISO 27001 certified[28] and offers robust security features to all customers, regardless of the geographical Region in which they store their content.

[28] http://aws.amazon.com/compliance/iso-27001-faqs/

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 is able to manage this responsibility.

A customer's AWS access keys can be used as an example to help explain why the customer rather than AWS is best placed to manage this responsibility.

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 and there are circumstances in which notifying individuals will be the best approach in order to mitigate risk, even though it is not mandatory under the applicable law. It is for the customer to determine when it is appropriate or necessary for them to notify individuals and the notification process they will follow.

Other considerations

This whitepaper does not discuss other Hong Kong laws, aside from the PDPO. 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 will 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 they identify and understand the requirements applying to them, and seek appropriate advice.

Closing Remarks

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

AWS services are designed to give customers flexibility over how they configure and deploy their solutions as well as control over 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.

Additional Resources

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 and http://aws.amazon.com/security.

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

European Union[29]
Germany[30]
Australia[31]
Singapore[32]
Japan[33]
Malaysia[34]
New Zealand[35]
Philippines[36]

Further Reading

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. We offer free instructional videos[37], self-paced labs[38], and instructor-led classes[39]. 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, please contact AWS at: https://aws.amazon.com/contact-us/ or contact your local AWS account representative.

[29] https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf
[30] https://d1.awsstatic.com/whitepapers/compliance/German_Data_Protection_Whitepaper.pdf
[31] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[32] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf
[33] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Japanese_Privacy_Considerations.pdf
[34] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[35] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[36] https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Philippines_Privacy_Considerations.pdf
[37] https://www.aws.training/
[38] https://aws.amazon.com/training/self-paced-labs/
[39] https://aws.amazon.com/training/course-descriptions/

Document Revisions

Date	Description
December 2017	First publication
May 2018	Second publication