# Using AWS in the Context of Malaysian Privacy Considerations

*January 2016*

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

# Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions, or assurances from AWS, its affiliates, suppliers, or licensors. 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.

# 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 key privacy considerations and the Personal Data Protection Act 2010 ("**PDPA**"). 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 the implications of the PDPA on 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 and the laws of other jurisdictions where that customer conducts business. This paper 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 more generally, applicable laws 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 information that a customer provides to us in connection with the creation or administration of its AWS account, 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.

# Customer Content: Considerations relevant to privacy

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 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 below:

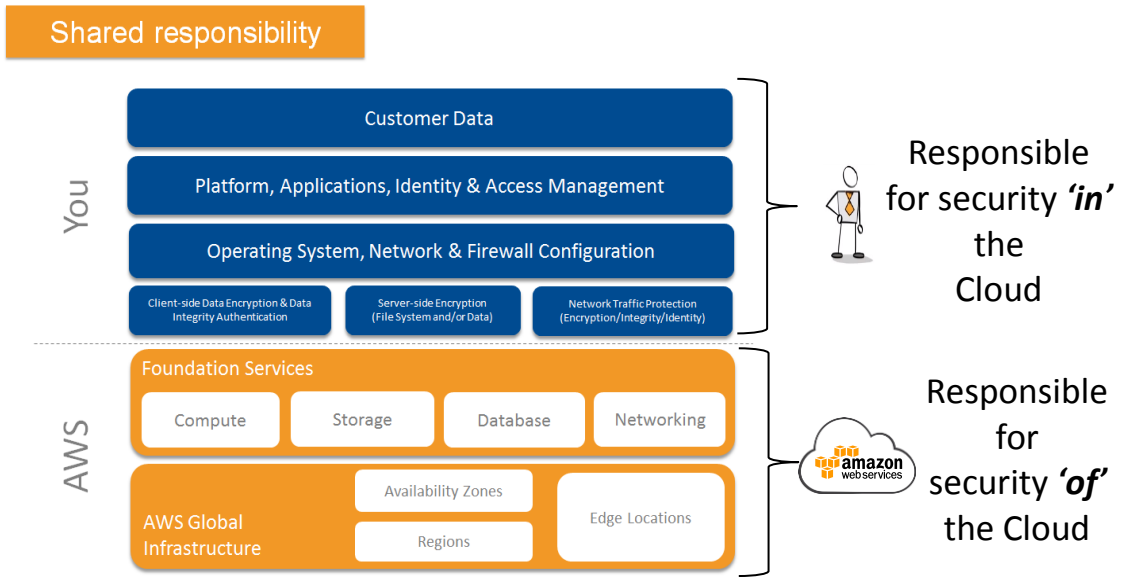


**Figure 1 – Shared Responsibility Model**

## 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, platform, 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 an extremely scalable, highly reliable platform that enables 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, platforms, and services, please read our Overview of Security Processes[1] 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 Service Organization Control (SOC) 1, 2[2] and 3[3] reports, ISO 27001[4], 27017[5] and 27018[6] certifications and PCI-DSS[7] compliance reports. These reports and certifications are produced by independent third party auditors and attest to the design and operating effectiveness of AWS security controls. Our 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content. AWS 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

[1] https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
[2] http://aws.amazon.com/compliance/soc-faqs/
[3] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[4] http://aws.amazon.com/compliance/iso-27001-faqs/
[5] http://aws.amazon.com/compliance/iso-27017-faqs/
[6] http://aws.amazon.com/compliance/iso-27018-faqs/
[7] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

standards can be found at 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 place in the AWS cloud, 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 tools enable 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 put on AWS, 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, platforms, 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 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 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.

# 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 a "Region". Customers have access to thirteen AWS Regions around the globe[8], including an Asia Pacific (Singapore) Region. Customers can choose to use one Region, all Regions or any combination of Regions. Figure 2 shows AWS Region locations:

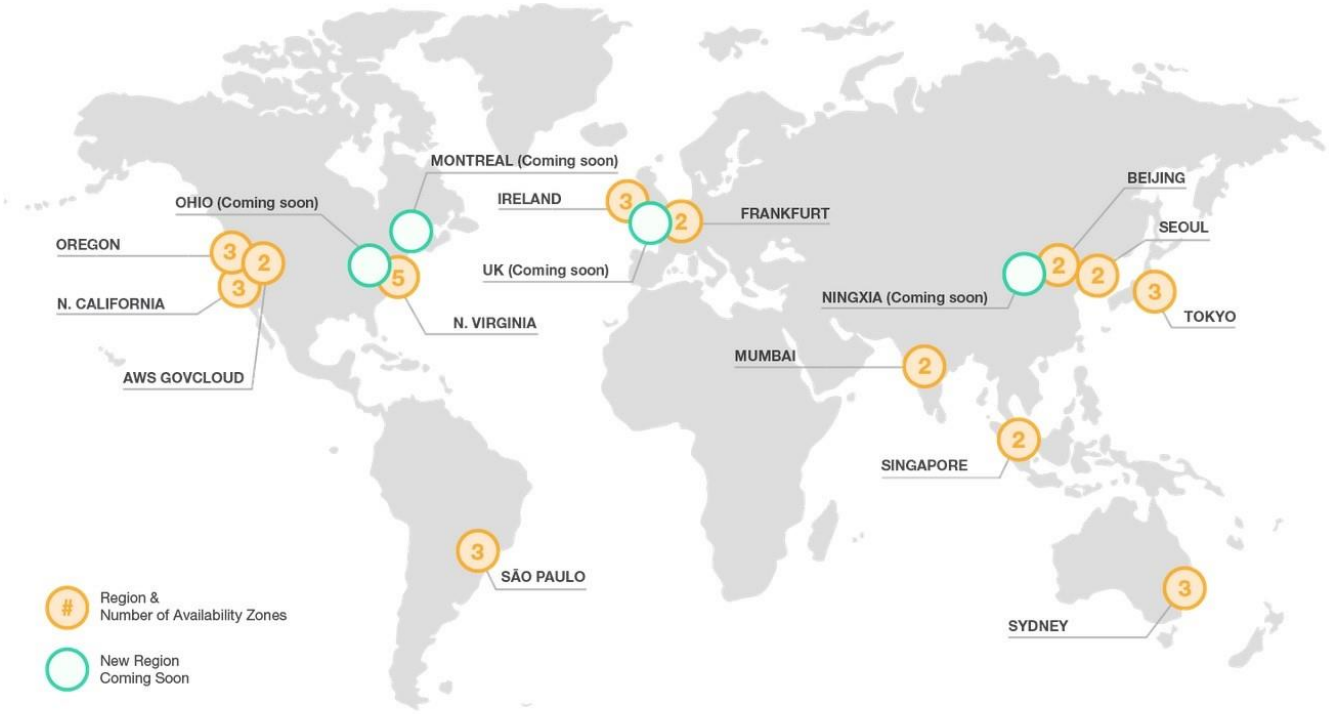


**Figure 2 – AWS Global Regions**

[8] 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.

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. AWS customers in Malaysia can choose to deploy their AWS services exclusively in one Region such as the Asia Pacific (Singapore) Region. If the customer makes this choice, their content will be located in Singapore unless the customer chooses to move that content.

Customers always retain control of which Region(s) are used to store and process content. AWS only stores and processes each customers' content in the Region(s), and using the services, chosen by the customer, and otherwise will not move customer content 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 Region or Regions where it wishes to use AWS services. Figure 3: Selecting AWS Global Regions provides an example of when uploading content to an AWS storage service or provisioning compute resources using the AWS management console.

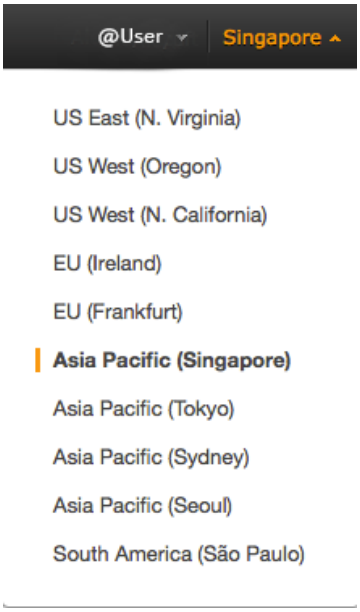


**Figure 3 – Selecting AWS Global Regions in the AWS Management Console**

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 into the VPC will only reside in the Region in which that VPC was created. For example, by creating a VPC in the Singapore Region and providing a link (either a VPN[9] or Direct Connect[10]) back to the customer's data center, all compute resources launched into that VPC would only reside in the Asia Pacific (Singapore) Region.

**Transfer of personal information cross border**

When using AWS services, customers may choose to transfer content containing personal information cross border, and they will need to consider the legal requirements that apply to such transfers. AWS can provide 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 under the EU Directive) from the EU to a country outside of the European Economic Area, such as Singapore. AWS has obtained approval from EU data protection authorities, known as the Article 29 Working Party, of the AWS Data Processing Addendum and Model Clauses. With our EU-approved Data Processing Addendum and Model Clauses, AWS customers—whether established in Europe or a Malaysian or global company with operations in the European Economic Area—can continue to run their operations using AWS in full compliance with the EU Directive. For additional information, please visit the AWS EU Data Protection FAQ. For more information on how customers can enter into the AWS Data Processing Addendum, please visit here (sign-in required).

# 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 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

[9] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
[10] http://aws.amazon.com/directconnect/

- 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 disposal.

### AWS access to customer content

AWS makes available to each customer the compute, storage, database, networking or other services selected by the customer, as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features, managing their own encryption keys, or using a third-party encryption mechanism of their own choice. AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. 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. However, it is important to remember that these laws all contain criteria that must be satisfied before authorizing access by the relevant government body. For example, the government agency seeking access will need to show it has a valid reason for requiring a party to provide access to content. Most importantly, access powers largely relate to law enforcement and counter-terrorism.

Many countries have data access laws which purport to apply extraterritorially. An example of a US 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 Malaysian companies doing business in the United States may find they are subject to 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-U.S. 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 the AWS services.

# Privacy and Data Protection in Malaysia

## The PDPA

This part of the paper discusses aspects of the Personal Data Protection Act 2010 ("**PDPA**") which came into force on 15 November 2013.

There are seven data protection principles which form the basis of protection under the PDPA, namely the General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle ("**Data Protection Principles**"). Data Protection Principles impose requirements for collecting, managing, dealing with, using, disclosing and otherwise handling personal data. The Data Protection Principles can be found at: http://www.kkmm.gov.my/akta_kpkk/Personal_Data_Protection_Act_2010.pdf.

The PDPA makes a distinction between a "data user" who processes any personal data or has control or authorizes the processing of any personal data, and a "data processor" who processes personal data solely on behalf of the data user, and does not process the personal data for any of his 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 data 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:

- 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 collected
- 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

Accordingly, in relation to personal data included in customer content stored in AWS, the Customer, rather than AWS, is the data user under the PDPA and is responsible for compliance with the requirements of the PDPA that apply to a data user. 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 those third parties.

We summarize below some requirements of the Data Protection Principles that are particularly important for a customer to consider if using AWS to store personal data. We also discuss aspects of the AWS services relevant to these requirements.

| Data Protection Principle | Summary of Data Protection Principle | Considerations |
|---|---|---|
| General Principle | Personal data can only be processed once the data subject has given his/her consent. | **Customer:** The customer has control of their content and knows if personal data is included in their content. Only the customer is able to communicate directly with data subjects whose personal data the customer stores in AWS about treatment of their personal data. The customer rather than AWS will know the scope of any consents obtained by the customer from data subjects, and the customer must ensure its use of the AWS services is consistent with these.<br><br>**AWS:** AWS does not collect personal data from the data subjects whose personal data is included in content the customer stores in AWS and AWS has no contact with them. Therefore, AWS is not required and unable in the circumstances to communicate with the relevant data subjects to seek any required consents. |
| Notice and Choice Principle | Data users must inform the data subject of the purposes for which their personal data is being collected and processed. | **Customer:** The customer is the data user and is responsible for meeting any Notice and Choice Principle requirement to notify data subjects whose personal data the Customer stores using AWS about all relevant matters required under the Notice and Choice Principle. This includes, if applicable, that the customer uses services provided by third parties such as AWS to store that personal data.<br><br>**AWS**: AWS does not know when a customer chooses to upload to AWS content that contains personal data. AWS also does not collect personal data from the data subjects whose personal data is included in content the customer stores in AWS. AWS is therefore not required and is unable in these circumstances to provide any notifications to the relevant data subjects. 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. |

| Data Protection Principle | Summary of Data Protection Principle | Considerations |
|---|---|---|
| Disclosure Principle | Personal data must only be disclosed with consent, and only for the purposes disclosed to the data subject. | **Customer:** The data user (Customer) is required to disclose to data subjects, the classes of third parties (e.g. service providers) that the customer discloses their personal data to, and the purposes for which the personal data is disclosed. Customers who transfer personal data to a place outside Malaysia, must also disclose this to, and obtain consent from, the data subject.[11] Where a customer has a geographical or regional constraint, for example where the customer has disclosed that content will be stored in a specific location, the customer can choose the AWS Region or Regions where their content will be stored to align to that location.<br><br>**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. AWS also does not move customer content from one Region to another, unless the customer chooses to do so.<br><br>**General:** The AWS service is structured so that a customer maintains effective control of customer content regardless of what AWS Region they use for their content. |
| Security Principle | A data user must take practical steps to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. | **Customers:** The Customer is the data user and is responsible for security ***in*** the cloud, including security of their content (and personal data included in their content).<br><br>**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, platforms, and services, please read our Overview of Security Processes[12] whitepaper. |
| Retention Principle | Personal data must not be kept longer | **Customers:** Customers are responsible for ensuring that personal data is deleted when no longer required. Only the |

[11] The PDPA provides for the Minister of Communications and Multimedia to also specify places outside of Malaysia where personal data may be transferred to (without such consent being required), however none have been specified at the date of this paper.

[12] for under the Personal Data Protection (Class of Data Users) Order 2013. The Minister of Communications and Multimedia, may also upon the recommendation of the Commissioner, specify additional classes of data users who will be required to be registered as data users under the PDPA.

| Data Protection Principle | Summary of Data Protection Principle | Considerations |
|---|---|---|
| | than necessary for the fulfilment of the purpose for which the personal data was collected. | customer knows when it no longer needs personal data it has stored in AWS, and therefore the Customer must manage deletion of the personal data at that point in time.<br><br>**AWS:** The AWS Services provide the customer with controls to enable the Customer to delete content, as described in the documentation available at http://aws.amazon.com/documentation. |
| Data Integrity Principle | The data user must take all reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up-to-date, having regard to the purpose for which the personal data was collected. | **Customers:** The customer is the data user. When a customer chooses to store content containing personal data using AWS, the customer has control over the quality of the personal data and has access to and can correct any personal data. 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.<br><br>**AWS**: AWS's SOC 1 Type 2 report includes controls that provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. |
| Access Principle | A data user must provide a data subject access to their personal data and they must be able to correct their personal data. | **Customers:** The Customer is the data user and therefore must provide data subjects whose personal data the Customer stores in AWS with access to their personal data, and the ability to correct their personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date (unless the PDPA provides for the customer to refuse a request). AWS does not access customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users.<br><br>**AWS:** The Customer rather than AWS collects personal data from the data subjects whose personal data is included in content the customer stores in AWS, and the Customer manages and controls who has access to customer content. AWS has no contact with data subjects. Therefore, AWS is not required and unable in the circumstances to provide such data subjects with access to their personal data. |

### Data User Registration

The PDPA makes it a requirement for specified classes of data users to

register with the Personal Data Protection Commissioner as data users.[13] Customers should determine whether they fall within any of the specified classes of data users that are required to register. AWS does not fall within any of the specified classes of data users that are required to be registered.

### Privacy Breaches

Given that customers maintain management and control of their data when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify affected individuals as required under applicable law.

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.

It is currently not a requirement of the PDPA to notify individuals of unauthorized access to or disclosure of their personal data. It is for the customer to determine when it is appropriate for them to notify individuals and the notification process they will follow.

### Other considerations

This whitepaper does not discuss other Malaysian privacy related laws, aside from the PDPA, that may also be relevant to customers, 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 it operates, 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 more than one million active customers 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.

[13] The specified classes of data users required to register with the Commissioner are as provided

## 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 are available for the following countries or regions:

Australia[14]
European Union[15]
Malaysia[16]
New Zealand[17]
Singapore[18]

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, 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 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.

[14] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[15] http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf
[16] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[17] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[18] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf