# Using AWS in the Context of Japan Privacy Considerations

First Published May 2018

Updated March 2022



#### **Notices**

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

#### Contents

Considerations relevant to privacy and data protection	2
The AWS Shared Responsibility approach to managing cloud security	3
Understanding security <i>OF</i> the cloud	4
Understanding security <i>IN</i> the cloud	5
AWS Regions: Where will content be stored?	7
How can customers select their Region(s)?	8
Transfer of personal data cross-border	10
Who can access customer content?	11
Customer control over content	11
AWS access to customer content	11
Government rights of access	11
AWS policy on granting government access	12
Privacy and data protection in Japan: The Act on the Protection of Personal Information	13
Privacy breaches	21
Consideration	22
Conclusion	22
Further reading	23
Document Revisions	24
Notes	24

### Abstract

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

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

#### Introduction

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

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

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

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



# Considerations relevant to privacy and data protection

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

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

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

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

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



# The AWS Shared Responsibility approach to managing cloud security

Will customer content be secure?

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

The customer generally connects to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections; they are part of the customer's area of responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. The respective roles of the customer and AWS in the shared responsibility model are shown in Figure 1:



Figure 1 – The AWS Shared Responsibility Model



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

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

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

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

#### Understanding security OF the cloud

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

AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which they store their content. 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 24 hours a day, seven days a week by trained security guards, and access is authorized strictly on a least privileged basis. For a complete list of all the security measures built into the core AWS cloud infrastructure, and services, see the Introduction to AWS Security whitepaper.

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

The AWS ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content. These reports and certifications are produced by independent third party auditors and attest to the design and operating effectiveness of AWS security controls. AWS compliance certifications and reports can be requested at <u>AWS Artifact</u>. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found on the



#### AWS Compliance site.

#### Understanding security IN the cloud

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

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

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

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

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

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

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices, and for security of the content they store or process using AWS services, or that they connect to their AWS infrastructure, such as the guest operating



system, applications on their compute instances, and content stored and processed in AWS storage, databases, or other services.

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

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

Subject to AWS policies regarding testing (see the Penetration Testing page), 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 <u>Penetration Testing</u> page.



# AWS Regions: Where will content be stored?

AWS data centers are built in clusters in various Regions. Each of these data center clusters in a given country is referred to an "AWS Region". Customers have access to a number of AWS Regions around the world, including an Asia Pacific (Tokyo) Region and an Asia Pacific (Osaka) Region. Customers can choose to use one Region, all Regions, or any combination of AWS Regions. Figure 2 shows AWS Region locations as of December 2021. For the most current information on AWS Regions, see the <u>Global Infrastructure</u> page.



Figure 2 – AWS Regions

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

Customers can use AWS services with the confidence that their data stays in the AWS Region that they select. <u>A small number of AWS services</u> involve the transfer of customer data, for example, 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(s)?

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

Figure 3 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 <u>AWS Management Console</u>.



<u>۵</u>	0	Global 🔺
US East (N. Virginia)		us-east-1
US East (Ohio)	ji ji	us-east-2
US West (N. California)		is-west-1
US West (Oregon)		is-west-2
Africa (Cape Town)	a	-south-1
Asia Pacific (Hong Kong)		ip-east-1
Asia Pacific (Jakarta)	ap-sou	itheast-3
Asia Pacific (Mumbai)	ар	-south-1
Asia Pacific (Osaka)	ар-по	rtheast-3
Asia Pacific (Seoul)	ар-по	rtheast-2
Asia Pacific (Singapore)	ap-sou	itheast-1
Asia Pacific (Sydney)	ap-sou	itheast-2
Asia Pacific (Tokyo)	ар-по	rtheast-1
Canada (Central)	ca-	central-1
Europe (Frankfurt)	eu-	central-1
Europe (Ireland)		u-west-1
Europe (London)	e	u-west-2
Europe (Milan)	eu	i-south-1
Europe (Paris)		u-west-3
Europe (Stockholm)	eu	-north-1
Middle East (Bahrain)	me	-south-1
South America (São Pau	lo)	sa-east-1

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 is located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Tokyo) Region and providing a link (either a <u>VPN</u> or <u>Direct Connect</u>) back to the customer's data center, all compute resources launched into that VPC would only reside in the Asia Pacific (Tokyo) 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 see the AWS General Data Protection Regulation (GDPR) Center and the <u>Navigating GDPR Compliance on AWS</u> whitepaper.

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

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



# Who can access customer content?

#### **Customer control over content**

AWS is vigilant about your privacy, and AWS provides the most flexible and secure cloud computing environment available today. With AWS, customers own their data, customers control the data location, and customers control who has access to it. AWS is transparent about how AWS services process the personal information customers upload to their AWS account (customer data), and AWS provides capabilities that allow customers to encrypt, delete, and monitor the processing of their data. Customers can:

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

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

#### AWS access to customer content

AWS makes available to each customer the compute, storage, database, networking, or other services, as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features (such as AWS KMS), managing their own encryption keys, or using a third party encryption mechanism of their own choice. AWS prohibits, and AWS systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by the customer, is required to prevent fraud and 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 content. The local laws that apply in the jurisdiction where the content is located are



an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice from their advisors to understand the application of relevant laws to their business and operations.

#### AWS policy on granting government access

AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, AWS notifies customers where practicable before disclosing their content so customers can seek protection from disclosure, unless AWS is legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the <u>Amazon Information Requests Portal</u> online.



# Privacy and data protection in Japan: The Act on the Protection of Personal Information

In Japan, the primary legislation dealing with data protection is the Act on the Protection of Personal Information (APPI) and its related regulations. The APPI<sup>1</sup> was most recently amended effective as of 20 December 2020, and a <u>further amendment</u> will come into effect on April 1, 2022. In addition, multiple guidelines have been issued to date by various government ministries for their respective industries, as well as by the <u>Personal Information</u> <u>Protection Commission (PPC)</u>, a government data protection authority.

APPI applies to business operators that provides goods or services in Japan and handle personal information of Japanese residents. Unlike many other countries, the APPI does not strictly distinguish between a data controller who has control over personal information and the purposes for which it can be used, and a data processor who processes information at the direction of and on behalf of a data controller. The APPI applies to all business operators (individuals and entities) that handle personal information database. The APPI also distinguishes between personal information and personal data. Under the APPI, personal data is personal information that is organized into database. Obligations on business operators vary depending on whether the business operators collect, use, or provide, personal information or personal data.

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:

- Collects 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 notification 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 the data protection principles of the APPI 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
Collection, notification and purpose of use	Business operators are prohibited from using deceptive or other improper means to collect personal information. Business operators must obtain the data subject's consent when collecting sensitive information <sup>2</sup> . When collecting personal information, business operators must promptly either notify the data subject or publicly announce the purpose of use of such personal information. The purpose of use must be specified in as much detail as possible, and any changes must be reasonable. Entities must not use the personal information beyond the scope necessary to achieve the purpose of use, unless they have obtained the prior consent of the data subject or are allowed to under an exemption in the APPI or other	<ul> <li>Customer: The customer determines and controls when, how and why it collects personal information from individuals, and decides whether it will include that personal information in customer content it stores or processes using the AWS services.</li> <li>The customer may also need to ensure it notifies or publicly announces the purposes for which it collects that data to the relevant data subjects, collects the data from a permitted source and it only uses the data for a permitted purpose.</li> <li>As between the customer and AWS, the customer has a relationship with the individuals whose personal information the customer stores on AWS, and therefore the customer is able to communicate directly with AWS about acquisition and treatment of their personal information.</li> <li>The customer rather than AWS also knows the scope of any notifications given to, or consents obtained by the customer from, such individuals whose personal information.</li> <li>AWS: AWS does not collect personal information from individuals whose personal information is included in content a customer stores or processes using AWS, and AWS has no contact with those individuals. Therefore, AWS is unable in these circumstances to communicate with the relevant individuals.</li> </ul>



Data protection principle	Summary of data protection obligations	Considerations
	applicable law.	AWS uses customer content only to provide the AWS services selected by each customer to that customer and does not use customer content for any other purposes without the customer's consent.
Maintaining the accuracy of personal data	Business operators must strive to ensure personal data (personal information constituting part of a	<b>Customer:</b> When a customer chooses to store personal information using AWS, the customer has control over the quality of that personal information, and the customer retains access to



Data protection principle	Summary of data protection obligations	Considerations
	personal information database) is always accurate and up to date.	and can correct it. This means that the customer must take all required steps to ensure that the personal information is accurate, complete, not misleading and kept up-to-date.
		<b>AWS</b> : AWS's <u>System &amp; Organization</u> <u>Control (SOC) 1 Type 2 report</u> includes controls that provide reasonable assurance that data integrity is maintained through all phases including transmission, storage, and processing.
Securing personal data	Business operators must take necessary and appropriate security measures for personal data.	<b>Customer:</b> Customers are responsible for security <b>in</b> the cloud, including security of their content (and personal information included in their content). As such, customers are required to take appropriate security measures for personal information stored in their customer content.
		Examples of steps customers can take to help secure their content include implementing strong password policies, assigning appropriate permissions to users and taking robust steps to protect their access keys, as well as appropriate firewalls and network segmentation, encrypting content, and properly architecting systems to decrease the risk of data loss and unauthorized access.
		<b>AWS:</b> AWS is responsible for managing the security <b>of</b> the underlying cloud environment. For a complete list of all the security measures built into the core AWS cloud infrastructure, and services, see the <u>Introduction to AWS Security</u>



Data protection principle	Summary of data protection obligations	Considerations
		whitepaper.
		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 and 3 reports, ISO 27001, 27017, and 27018 certifications, and PCI DSS Attestation of Compliance.
Transferring personal information to third parties	Business operators generally must obtain consent from the data subjects to transfer their personal data to third parties unless they fall under certain exemptions.	<b>Customer:</b> The customer should consider whether it is required to obtain any consents from the relevant individuals relating to the transfer of personal information to a third party. As between the customer and AWS, the customer has a relationship with the individuals whose personal information is stored by the customer on AWS, and therefore the customer is able to communicate directly with them about such matters.
		<b>AWS:</b> AWS does not collect personal information from content that a customer stores or processes using AWS, and AWS has no contact with individuals whose personal information is stored by the customer on AWS. Therefore, AWS is not required and is unable in the circumstances to communicate with the relevant individuals to seek any required consents for transfer.
Storing personal information on a cloud service provider	According to section 7-53 of <u>2017 Q&amp;As</u> (updated in 2021) issued by the PPC, provision of personal data by an entity to a cloud service is not	<b>Customer:</b> The customer determines and controls when, how and why it collects personal information from individuals, and decides whether it will include that personal information in customer content it stores or processes using the AWS services.



Data protection principle	Summary of data protection obligations	Considerations
	considered a (i) transfer requiring data subject consent or (ii) entrusting of personal data requiring monitoring, unless the cloud service provider handles the personal data stored on its server.	The customer should consider whether it is required to take any measures under applicable privacy law in connection with the storing of personal information on a cloud service provider. According to section 7-53 of <u>2017</u> <u>Q&amp;As (updated in 2021)</u> issued by PPC, storing or processing of content using AWS will not be considered a transfer or entrusting of personal data to AWS, unless the customer and AWS agree that AWS will handle personal data stored in such content. <b>AWS:</b> AWS does not collect personal information from content that a customer stores or processes using AWS, and AWS has no contact with individuals whose personal information is stored by the customer on AWS. Therefore, AWS does not handle personal information stored on its server unless the customer and AWS agree to do so.
Restrictions on international transfer of personal data	Business operators may only transfer personal data to a foreign country when such country has a legal system that is deemed equivalent to the Japanese system for protection of personal information, or where the data is transferred to an overseas third party that undertakes adequate	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 the Asia Pacific (Tokyo) or Asia Pacific (Osaka) Region if preferred. The customer should consider whether it should disclose to individuals the locations in which it stores or processes their personal information and obtain any required consents relating to such locations from the relevant individuals if necessary. The



Data protection principle	Summary of data protection obligations	Considerations
	precautionary measures for the protection of personal data.Otherwise, business operators must obtain the data subject's consent to 	customer is responsible for ensuring compliance with applicable laws, including privacy laws wherever their content is located. As between the customer and AWS, the customer has a relationship with the individuals whose personal information the customer stores on AWS, and therefore the customer is able to communicate directly with them about such matters. <b>AWS:</b> AWS enables customers to use AWS services with the confidence that their customer data stays in the AWS Region customers select. <u>A small</u> <u>number of AWS services</u> such as a content delivery service. AWS is <u>ISO/IEC 27001</u> certified and offers robust security features to all customers, regardless of the geographical Region in which they store their content.



Data protection	Summary of data	Considerations
principle	protection obligations	Considerations
	international data transfer, unless the foreign cloud service provider handles the personal data stored on its server.	
Record keeping and confirmation of transfers of personal data to third parties	Business operators must confirm and record certain information prescribed by PPC relating to inbound and outbound transfers of personal data involving third parties.	<ul> <li>Customer: Customers are responsible for confirming and recording certain information prescribed by PPC relating to personal information that is received from, or provided to, third parties in order to ensure the traceability of such transfers of personal information.</li> <li>AWS: AWS cannot confirm or record information relating to transfers of personal information (if any) is uploaded by the customer, or if the customer transfers a personal information to a third party.</li> </ul>
Disclosure relating to retained personal data	Business operators handling retained personal data must make appropriate disclosures regarding how they handle retained personal information, normally in a privacy notice. For example, the following information available to data subjects for the purposes of handling complaints: (i) the business operator's name; (ii) the purpose of use of retained personal information; (iii) the	Customer: The customer is responsible for meeting these disclosure requirements to individuals whose personal information the customer is storing on AWS. AWS: AWS does not know when a customer chooses to upload content to AWS that may contain personal information. AWS also does not acquire personal information from individuals whose personal information is stored in AWS by AWS customers. AWS is unable, in these circumstances, to provide any required information to the relevant individuals.



Data protection principle	Summary of data protection obligations	Considerations
	procedures a data subject may use to request the entity to disclose, correct and discontinue using the personal information it possesses; and (iv) the business operator's contact information.	
Disclosure, correction and deletion	Business operators must disclose retained personal data to data subjects upon their request. Business operators must correct incorrect retained personal data if a data subject makes such a demand for correction. Business operators may be required to	<b>Customers:</b> When a customer chooses to store content containing retained personal information using AWS, the customer has control over the content and retains access and can correct or discontinue use of such retained personal information. This means that the customer must take all required steps to ensure that the personal information included in customer content is accurate, complete, not misleading and kept up to date.
	discontinue use of retained personal data if they are found to have violated the purpose of use.	<b>AWS</b> : 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 <u>AWS Documentation</u> .

# **Privacy breaches**

Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify



regulators and affected individuals as required under applicable law. Only the customer can to manage this responsibility.

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

The <u>amendment of APPI</u> that will take effect in April 2022 requires business operators to notify individuals in the event of certain material unauthorized access or disclosure of personal information. In some jurisdictions it is mandatory to notify individuals or a regulator of unauthorized access to or disclosure of their personal information. 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 white paper does not discuss other Japanese privacy laws, aside from the APPI, that may also be relevant to customers, including prefectural ordinances and industry specific requirements. The relevant privacy and data protection laws and regulations applicable to individual customers depend on several factors, including where a customer conducts business, the industry in which they operate, the type of content they wish to store, where or from whom the content originates, and where the content will be stored.

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

## Conclusion

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

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



# Further reading

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

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

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

Common Consideration California European Union Germany Australia Hong Kong Malaysia New Zealand Philippines Singapore South Africa

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 <u>free instructional videos</u>, <u>self-paced labs</u>, and <u>instructor-led classes</u>.

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

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: <u>https://aws.amazon.com/contact-us/</u> or contact your local AWS account representative.



## **Document Revisions**

Date	Description
December 2017	First publication
May 2018	Second publication
February 2022	Third publication

### Notes

<sup>1</sup> The original text is available at: <u>elaws.e-gov.go.jp</u> English translation of 2015 version of APPI is available at: <u>Japanese law translation project</u>

<sup>2</sup> Under APPI, sensitive information is personal information containing descriptions requiring special consideration in handling so as to avoid any unfair discrimination, prejudice or other disadvantage to an individual based on a person's race, belief, social status, medical history, criminal records, or the fact that a person has suffered damage through a criminal offense, etc.

