Using AWS in the Context of Australian Privacy Considerations

March 2018

(Please consult https://aws.amazon.com/compliance/aws-whitepapers/ 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 information, in the context of key privacy considerations and the Australian Privacy Act 1988 (Cth). 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 Australian Privacy Act on their use of AWS services to store or process content containing personal information. 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 information 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[1].

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

Customer Content: Considerations relevant to privacy

Storage of content presents all organisations 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, anonymised 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 virtualisation 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:

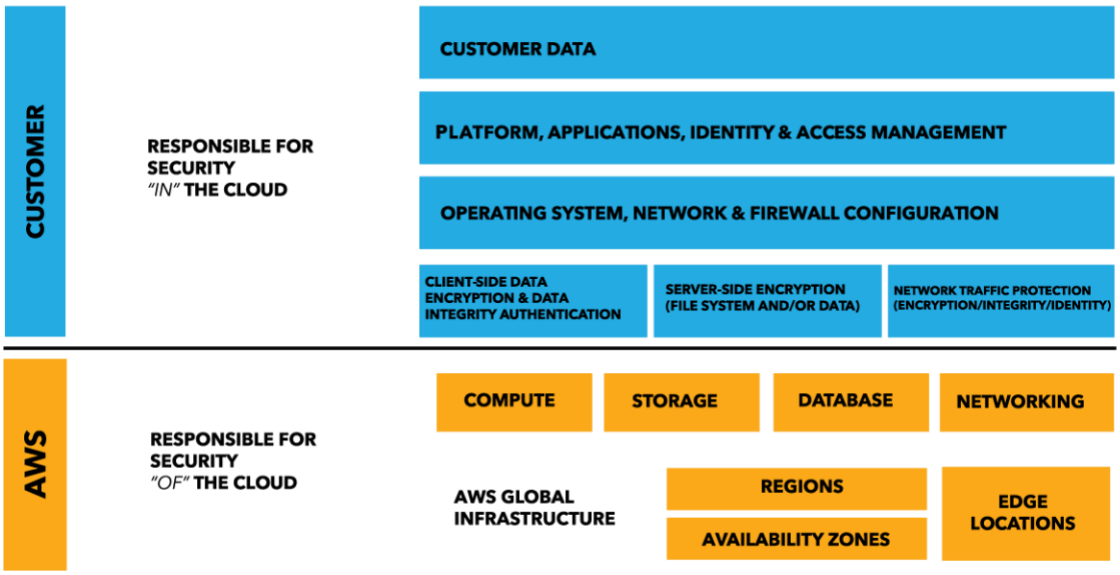

Figure 1 – Shared Responsibility Model

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, platform, applications, systems and networks – no differently than they would for applications in an on-site data centre.

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 centres utilise state-of-the art electronic surveillance and multi-factor access control systems. Data centres are staffed 24x7 by trained security guards, and access is authorised 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[2] whitepaper.

We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorised access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Systems & Organization Control (SOC) 1, 2[3] and 3[4] reports,

[2] https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
[3] http://aws.amazon.com/compliance/soc-faqs/
[4] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

ISO 27001[5], 27017[6] and 27018[7] certifications and PCI DSS[8] 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. AWS's 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://pages.awscloud.com/compliance-contact-us.html. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found at AWS's compliance site[9].

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

[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/pci-dss-level-1-faqs/
[9] https://aws.amazon.com/compliance/

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 unauthorised 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 organisation'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[10].

[10] http://aws.amazon.com/aup/

AWS Regions: Where will content be stored?

AWS data centres are built in clusters in various global regions. We refer to each of our data centre clusters in a given country as a "Region." Customers can choose to use one Region, all Regions or any combination of Regions. Figure 2 shows AWS Region locations as at March 2018[11].

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 (2)

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)

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

Figure 2 – AWS Global Regions

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 of their choice. AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) Region and store their content onshore in Australia. If the customer makes this choice, their content will be located in Australia 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.

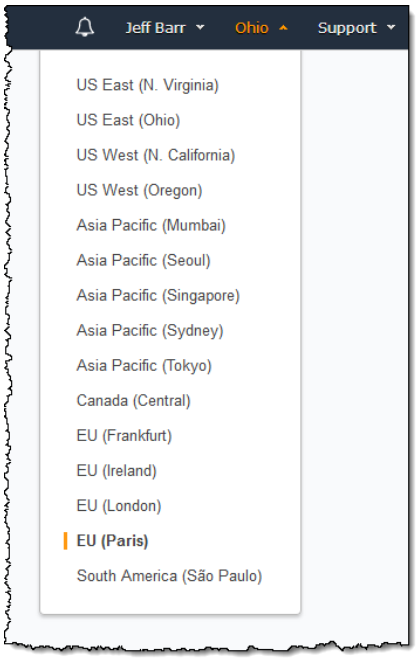

Figure 3 – Selecting AWS Global Regions in the AWS Management Console

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 centre.

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 Sydney region and providing a link (either a VPN or Direct Connect) back to the customer's data centre, all compute resources launched into that VPC would only reside in the Asia Pacific (Sydney) 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 Australia. 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 an Australian 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[12]. For more information on how customers can enter into the AWS Data Processing Addendum, please visit our web page[13] (sign-in required).

In 2016, the European Commission approved and adopted the new General Data Protection Regulation (GDPR). The GDPR will replace the EU Data Protection Directive, as well as all local laws relating to it. All AWS services will comply with the GDPR when it becomes enforceable on May 25, 2018. AWS provides customers with services and resources to help them comply with GDPR requirements that may apply to their operations. These include AWS's adherence to the Cloud Infrastructure Services Providers in Europe code of conduct, granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards and AWS's C5 attestations. For additional information, please visit the AWS General Data Protection Regulation (GDPR) Center[14], and our Navigating GDPR Compliance on AWS Whitepaper[15].

[12] https://aws.amazon.com/compliance/eu-data-protection/
[13] https://aws.amazon.com/compliance/eu-data-protection/console/dpa
[14] https://aws.amazon.com/compliance/gdpr-center/
[15] 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 Region) of that storage
- Control the format, structure and security of their content, including whether it is masked, anonymised 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 disposal.

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, 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.

Australia, like most countries, has legislation that enables Australian law enforcement and government security bodies to seek access to information; for example the *Australian Security Intelligence Organisation Act 1979* (Cth)[16]

There is also the ability for foreign law enforcement bodies to apply for access to information in Australia through legislation that gives effect to mutual assistance treaties between many countries and Australia[17]. However, it is important to remember that these laws all contain criteria that must be satisfied before authorising 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 centre or in physical records. This means that Australian companies doing 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 Australian, 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 recognised 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

[16] http://www.comlaw.gov.au/Details/C2012C00260
[17] Mutual Assistance in Criminal Matters Act 1987 (Cth)

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[18].

Privacy and Data Protection in Australia: The Privacy Act

This part of the paper discusses aspects of the Australian *Privacy Act 1988* (Cth) applying from 12 March 2014 when a number of changes took effect.

From 12 March 2014, the main requirements in the Privacy Act for handling personal information are set out in the Australian Privacy Principles (APPs). The APPs, impose requirements for collecting, managing, dealing with, using, disclosing and otherwise handling personal information.

The APPs can be found at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/app- quick-reference-tool.

Unlike other privacy regimes, the APPs do not distinguish between a "data controller" who has control over personal information and the purposes for which it can be used, and a "data processor" that processes information at the direction of and on behalf of a "data controller." The APPs do however apply in different ways to different types of entities. For example, the way the APP requirements apply to each organisation depends on the role they play in relation to the relevant personal information. Obligations vary depending on whether they "collect", "use", "transfer" or "disclose", personal information.

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 its end users, and determines the purpose for which the customer requires and will use the information
- Has the capacity to control who can access, update and use the personal information collected
- Manages the relationship with the individual about whom the personal information relates, including by communicating 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

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

responsibilities, but the customer, rather than AWS, would manage its relationships with those third parties.

We summarise in the table below some APP requirements particularly important for a customer to consider if using AWS to store personal information. We also discuss aspect of the AWS Services relevant to these APPs.

APP	Summary of APP requirements	Considerations
APP 1.2	An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities to ensure compliance with the APPs and to enable the entity to deal with inquiries or complaints about compliance with the APPs.	The APPs apply differently to each party, reflecting the level of control and access each party has over the personal information. **Customer:** The APPs will impose more extensive obligations on the customer than AWS. This is because the customer has control of their content and is able to communicate directly with individuals about treatment of their personal information. **AWS:** To the extent the APPs may apply to AWS they would apply in a more limited way. As explained above, the customer rather than AWS knows 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.
APP 1.3 - 1.6	An entity must maintain a privacy policy addressing particular matters about how the entity manages personal information and comply with requirements for making that policy available.	**Customer:** Customers are responsible for maintaining their own privacy policy that complies with the APPs. **AWS:** In the context of customer content, AWS does not know what content is uploaded by the customer and does not control that content. For this reason, our privacy policy cannot address how each

APP	Summary of APP requirements	Considerations
		customer chooses to use personal information included in their customer content. However, customers may provide information to AWS in connection with the creation or administration of AWS accounts. The AWS Privacy Policy describes how AWS collects and uses account information that it receives.
APP 5	Where an entity collects personal information about an individual, the entity must take such steps as are reasonable in the circumstances to tell or otherwise ensure the individual is aware of certain matters.	**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. The customer may also need to ensure it discloses the purposes for which it collects that data to the relevant data subjects, obtains the information from a permitted source and that it only uses the information for a permitted purpose. 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 collection and treatment of their personal information. 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 information.

APP	Summary of APP requirements	Considerations
		Consequently the customer is responsible for meeting any APP requirement to notify individuals whose personal information the customer is storing on AWS about all relevant matters required under APP5, including, if applicable, about the customer's use of AWS to store that personal information. **AWS:** AWS does not know when a customer chooses to upload to AWS content that may contain personal information. AWS also 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 not required and is unable in the circumstances to communicate with the relevant individuals. AWS only uses customer content to provide the AWS services and does not use customer content for any other purpose.
APP 6	Rules about the circumstances in which an entity that collects personal information may use or disclose the personal information that it holds.	**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. If the customer chooses to include personal data in customer content stored in AWS, the customer controls the format and structure of its content and how it is protected from disclosure to unauthorised

APP	Summary of APP requirements	Considerations
		parties including whether it is anonymised or encrypted. The customer will know whether it uses the AWS services to store or process customer content containing personal data, and therefore is best placed to inform individuals that it will use AWS as a service provider, if required. **AWS:** AWS 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.
APP 8	Rules about disclosing personal information to an overseas recipient and exceptions to those rules.	**Customer:** The customer can choose the AWS Region or Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single Region if preferred, including maintaining their content in Australia, if required. 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 information 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 information the customer stores on AWS, and therefore the customer is able to

APP	Summary of APP requirements	Considerations
		communicate directly with them about such matters. **AWS:** AWS only stores and processes customer content in the Region(s), and using the services, each customer chooses, and otherwise will not move customer content except as legally required. If a customer chooses to store content in more than one Region, or copy or move content between Regions, that is solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed. **General:** It is important to highlight that an entity is only required to comply with APP 8 if there is a "disclosure" by that entity to an overseas recipient. The Office of the Information Commissioner (OAIC) has said disclosure generally occurs when an entity releases personal information from its effective control. 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. OAIC guidance indicates that information provided to a cloud service provider subject to adequate security and strict user control may be a "use" by the customer and not a "disclosure". Accordingly, using AWS services to store personal information outside Australia at

APP	Summary of APP requirements	Considerations
		the choice of the customer may be a "use" not a "disclosure" of customer content. Customers should seek legal advice regarding this if they feel it may be relevant to the way they propose to use the AWS Services.
APP 10 - 12	Rules about protecting the integrity of personal information including its quality, security and allowing access and corrections and destroying or de-identifying it.	Customers: Customers are responsible for their content and for security in the cloud. When a customer chooses to store or process content containing personal information 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 information included in customer content is accurate, complete, not misleading and kept up-to-date. In addition, as between the customer and AWS, the customer has a relationship with the individuals whose personal information 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. Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is

APP	Summary of APP requirements	Considerations
		no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymise the personal data when no longer needed. **AWS:** AWS is responsible for security of the underlying cloud environment. 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. 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 whitepaper[19]. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Systems & Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI-DSS compliance reports. 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 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

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

APP	Summary of APP requirements	Considerations
		required, and is unable in the circumstances, to provide such individuals with access to, or the ability to correct, their personal data. 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.

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

The Privacy Act introduced a new Australian notifiable data breaches (NDB) scheme, which came into force on February 22, 2018. AWS offers an Australian Notifiable Data Breaches (ANDB) Addendum to customers who are subject to the Privacy Act and are using AWS to store and process personal information covered by the NDB scheme. The ANDB Addendum addresses customers' need for notification if a security event affects their data. AWS has made the ANDB Addendum available online as a click-through agreement in AWS Artifact (the customer-facing audit and compliance portal that can be accessed from the AWS management console), where customers can review and activate the ANDB Addendum for AWS accounts they use to store and process personal information covered by the NDB scheme. The ANDB Addendum must be separately accepted for each AWS account that a customer requires to be covered.

Other considerations

This whitepaper does not discuss other Australian privacy laws, aside from the Privacy Act, that may also be relevant to customers, including state based laws and 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 Australian 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.

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[20]
- European Union[21]
- Malaysia[22]
- New Zealand[23]
- Singapore[24]

AWS Artifact

Customers can review and download reports and details about more than 2,500 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to

[20] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[21] https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf
[22] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[23] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[24] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf

AWS' security and compliance documents, including the ANDB Addendum and certifications from accreditation bodies across geographies and compliance verticals.

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[25], self-paced labs[26], and instructor led classes[27]. 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 https://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.

[25] https://www.aws.training/
[26] https://aws.amazon.com/training/self-paced-labs/
[27] https://aws.amazon.com/training/course-descriptions/