Using AWS in the Context of New Zealand Privacy Considerations

First published September 2014

Updated August 17, 2021

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.

Contents

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 considerations and the New Zealand Privacy Act 2020 (NZ). 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 services.

Introduction

This whitepaper focuses on typical questions asked by AWS customers when they are considering the implications of the New Zealand 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, or contractual commitments a customer makes to a third party.

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

When we refer to content in this paper, we mean software (including virtual machine images), data, text, audio, video, images and other content that a customer, or any end user, stores or processes using AWS services. For example, a customer's content includes objects that the customer stores using Amazon Simple Storage Service (Amazon S3), files stored on an Amazon Elastic Block Store (Amazon EBS) 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 accounts, such as a customer's names, phone numbers, email addresses and billing information—we refer to this as account information and it is governed by the AWS Privacy Notice. Our business changes constantly, and our Privacy Notice may also change. We recommend checking 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 AWS Region or Regions where their content is stored.
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted.
- Who has access to their AWS accounts and content, and how those access rights are granted, managed, and revoked.

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

AWS shared responsibility approach to managing cloud security

How is customer content secured?

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have important roles in the operation and management of security. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate.

The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS-provided security group firewall and other security-related features.

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

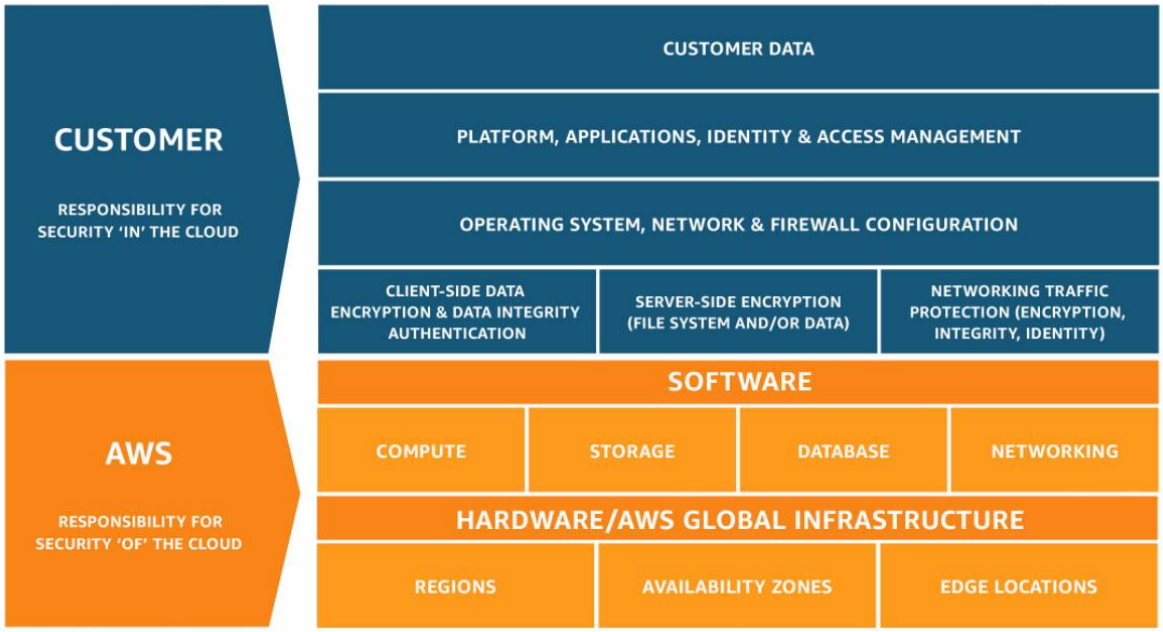

Figure 1 – AWS Shared Responsibility Model

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 on-site data center.

Understanding security OF the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS Cloud infrastructure has been architected to be one of the most flexible and

secure cloud computing environments available, designed to provide optimum availability while providing complete customer segregation. It provides extremely scalable, highly reliable services that enable customers to deploy applications and content quickly and securely, at massive global scale if necessary.

AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical Region in which they store their content. AWS' world-class, highly secure data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. For a complete list of all the security measures built into the core AWS Cloud infrastructure, and services, see Best Processes for Security, Identity, & Compliance.

We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System & Organization Control (SOC) 1, 2[1] and 3[2] reports, ISO 27001[3], 27017[4], 27018[5], and 9001[6] certifications and PCI DSS[7] Attestation of Compliance. Our ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content.

These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls. AWS compliance certifications and reports can be requested on the AWS Compliance Contact Us page. For more information on AWS compliance certifications, reports, and alignment with best practices and standards, see AWS Compliance.

Understanding security IN the cloud

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

Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change

customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures will be implemented in the cloud, in accordance with each customer's business needs.

For example, if a higher availability architecture is required to protect customer content, the customer may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to customer content is required, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.

To assist customers in designing, implementing, and operating their own secure AWS environment, AWS provides a wide selection of security tools and features customers can use. Customers can also use their own security tools and controls, including a wide variety of third-party security solutions. Customers can configure their AWS services to leverage a range of such security features, tools, and controls to protect their content, including sophisticated identity and access management tools, security capabilities, encryption, and network security. Examples of steps customers can take to help secure their content include implementing:

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

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices, and for security of the content they store or process using AWS services, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, databases, or other services.

AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service (AWS KMS) and AWS CloudTrail. 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 whitepapers relating to security, governance, risk and compliance; and a number of checklists and best practices. Customers are also free to design and conduct

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 an AWS Region. Customers have access to a number of AWS Regions around the world[8], including an Asia Pacific (Sydney) Region. Customers can choose to use one Region, all Regions or any combination of AWS Regions. Figure 2 shows AWS Region locations as of April 2021.[9]

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 or locations of their choice. For example, AWS customers in New Zealand can choose to deploy their AWS services exclusively in one AWS Region such as the Asia Pacific (Sydney) Region and store their content onshore in Australia, if this is their preferred location. If the customer makes this choice, AWS will not move their content from Australia without the customer's consent, except as legally required.

Customers always retain control of which AWS Regions are used to store and process content. AWS only stores and processes each customer's content in the AWS Region(s), and using the services, chosen by the customer, and otherwise will not move customer content without the customer's consent, except as legally required.

How can customers select their Region(s)?

When using the AWS Management Console, or in placing a request through an AWS Application Programming Interface (API), the customer identifies the particular AWS Region(s) where they want 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 AWS Management Console.

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

Customers can prescribe the AWS Region to be used for their AWS resources. Amazon Virtual Private Cloud (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 resources launched by the customer into the VPC will be located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Sydney) Region, all resources launched into that VPC would only reside in the Asia Pacific (Sydney) Region. This option can also be leveraged for other AWS Regions.

Transfer of personal information 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 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 Cloud Computing Compliance Controls Catalogue (C5) attestations. For additional information, visit the AWS General Data Protection Regulation (GDPR) Center and see the *Navigating GDPR Compliance on AWS* whitepaper.

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 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 (EEA).

With our EU Data Processing Addendum and Model Clauses, AWS customers who want to transfer personal data—whether established in Europe or a global company operating in the European Economic Area—can do so with the knowledge that their personal data on AWS will be given the same high level of protection it receives in the EEA. 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

Customers using AWS maintain and do not release effective control over their content within the AWS environment. Customers can perform the following:

- 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 enables 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 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 such as, AWS KMS, managing their own encryption keys, or using a third-party encryption mechanism of their own choice. AWS does not access or use customer content without the customer's consent, except as legally required. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Government rights of access

Queries are often raised about the rights of domestic and foreign government agencies to access content held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also

need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice to understand the application of relevant laws to their business and operations.

AWS policy on granting government access

AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law.

Non-governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the Law enforcement Information Requests page.

Privacy and data protection in New Zealand: The Privacy Act

This section discusses aspects of the New Zealand Privacy Act 2020 (NZ) (Privacy Act) effective from December 1, 2020.

The main requirements in the Privacy Act for handling personal information are set out in the Information Privacy Principles (IPPs). The IPPs impose requirements for collecting, managing, using, disclosing, and otherwise handling personal information collected from individuals in New Zealand. The New Zealand Privacy Commissioner may also issue codes of practice which apply, prescribe, or modify the application of IPPs in relation to an activity, industry, or profession (or classes of them).

The Privacy Act recognizes a distinction between “principals” and “agents”. Where an entity (the *agent*) holds personal information for the sole purpose of storing or processing personal information on behalf of another entity (the *principal*) and does not use or disclose the personal information for its own purposes, the information is deemed to be held by the *principal*. In those circumstances, primary responsibility for compliance with the IPPs will rest with the *principal*.

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 or processed using 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.
- 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.
- Transfers the content into the AWS Region it selects. AWS does not receive customer content in New Zealand.

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 in the following table the IPP requirements that are particularly important for customers to consider if using AWS to store personal information collected from individuals in New Zealand. We also discuss aspects of the AWS services relevant to these IPPs.

Table 1 — IPP requirements and considerations

IPP	Summary of IPP requirements	Considerations
IPP 1 – Purpose of collection of personal information	Personal information may be collected only for lawful and necessary purposes.	**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
IPP 2 – Source of personal information	Personal information may only be collected directly from the individual, unless an exception applies.	

IPP 3 – Collection of Information	Reasonable steps must be taken to ensure that when an individual's personal information is collected, they are aware of the purposes for which it is collected and certain other matters.	customer content it stores or processes using AWS services. The customer may also need to ensure it discloses the purposes for which it collects personal information to the relevant individuals; obtains the personal information from a permitted source; and, that it only uses the personal 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 or processes on AWS, and therefore the customer is able to communicate directly with them about collection 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. **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 the AWS services, and AWS has no
IPP 4 – Manner of collection of personal information	Personal information may only be collected fairly, and in a lawful and non-intrusive manner.	

		contact with those individuals. Therefore, AWS is not required and is unable in the circumstances to communicate with the relevant individuals. AWS only accesses or uses customer content as necessary to provide the AWS services and does not access or use customer content for any other purpose without the customer's consent.
IPP 5 – Storage and security of personal information	Reasonable steps must be taken to protect the security of personal information.	**Customer** — Customers are responsible for security in the cloud, including security of their content (and personal information included in their content). **AWS** — AWS is responsible for managing the security of the underlying cloud environment. For a complete list of all the security measures built into the core AWS Cloud infrastructure and services, see Best Practices for Security, Identity, & Compliance.
IPP 6 – Access to personal information	Individuals are entitled to access personal information about them, unless an exception applies.	**Customer** — Customers are responsible for their content in the cloud. When a customer chooses to store or process content containing personal information using the AWS services, the customer has control over the quality of that content and the customer retains access to and can correct it.
IPP 7 – Correction of personal information	Individuals may request correction of personal information about them.	

		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 the AWS services. Therefore, the customer, rather than AWS, is able to work with relevant individuals to provide them access to, and the ability to correct, their personal information. **AWS** — AWS uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes without the customer's consent. AWS has no contact with the individuals whose personal information is included in content a customer stores or processes using the AWS services. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to provide such individuals with access to, or the ability to correct, their personal information.
IPP 8 - Accuracy to be checked before use or disclosure	Reasonable steps must be taken to check accuracy, completeness, and relevance of personal information before it is used or disclosed.	**Customer** — When a customer chooses to store or process content containing personal information using the AWS services, 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. **AWS** — AWS does not collect personal information from individuals whose personal information is included in content a customer stores or processes using the AWS services, and AWS has no contact with those individuals. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to confirm the accuracy, completeness, and relevance of personal information before it is used or disclosed.
IPP 9 - Personal information must not be kept longer than necessary	Personal information should not be kept for longer than is required for the purposes for which the information may be lawfully used.	**Customer** — Because only the customer knows the purposes for collecting the personal information contained in the customer content it stores or processes using AWS services, the customer is responsible for ensuring that such personal information is not kept for longer than required. The customer should delete the personal information when it is no longer needed. **AWS** — AWS services provide the customer with controls to enable the customer to delete content

		stored on AWS, as described in AWS documentation.
IPP 10 - Limits on use of personal information **IPP 11 - Limits on disclosure of personal information**	Personal information may only be used or disclosed for the purpose for which it was collected, for reasonable directly related purposes, in a way which does not identify the individual, or if another exception applies.	**Customer** — Given that the customer determines the purpose for collecting personal information, and controls the use and disclosure of content that contains personal information, the customer is responsible for ensuring how such personal information is used or disclosed. The customer also controls the format, structure, and security of its content stored or processed using AWS services. **AWS** — AWS uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes without the customer's consent. **General** — AWS services are structured such that customers maintain ownership and control of their content when using the AWS services, regardless of which AWS Region they use.
IPP 12 – Disclosure of personal information outside New Zealand	Personal information may only be disclosed outside of New Zealand if the recipient is subject to similar safeguards to those under the Privacy Act.	**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 AWS Region if preferred. AWS services are structured so that a customer maintains effective control of customer content regardless of what AWS 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 is included in customer content stored or processed using the AWS services, and therefore the customer is able to communicate directly with them about such matters. **AWS** — AWS only stores and processes each customer's content in the AWS Region(s), and using the services chosen by that customer, and otherwise will not move customer content without that customer's consent, except as legally required. If a customer chooses to store content in more than one AWS Region, or copy or move content between AWS 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 IPP 12 when that entity discloses personal information to an overseas person or entity. The Privacy Act states that where an agency (Entity A),

		holds information as an agent for another agency (Entity B) - for example for safe custody or processing - then (i) the personal information is to be treated as being held by Entity B and not Entity A, (ii) the transfer of the information to Entity A by Entity B is not a use or disclosure of the information by Entity B, and (iii) the transfer of the information, and any information derived from the processing of that information, to Entity B by Entity A is not a use or disclosure of the information by Entity A. It also does not matter whether Entity A is outside New Zealand or holds the information outside New Zealand. Using the AWS services to store or process personal information outside New Zealand at the choice of the customer may not be 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.

Privacy breaches

Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.

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

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

The Privacy Act introduced a notifiable privacy breach scheme that is effective from December 1, 2020. The scheme aims to give affected individuals the opportunity to take steps to protect their personal information following a privacy breach that has caused, or is likely to cause, serious harm. AWS offers two types of New Zealand Notifiable Data Breaches (NZNDB) Addenda to customers who are subject to the Privacy Act and are using AWS to store and process personal information covered by the scheme.

The NZNDB Addenda address customers' need for notification if a security event affects their data. The first type, the Account NZNDB Addendum, applies only to the specific individual account that accepts the Account NZNDB Addendum. The Account NZNDB Addendum must be separately accepted for each AWS account that a customer requires to be covered. The second type, the Organizations NZNDB Addendum, once accepted by a management account in AWS Organizations, applies to the management account and all member accounts in that AWS Organization. If a customer does not need or want to take advantage of the Organizations NZNDB Addendum, they can still accept the Account NZNDB Addendum for individual accounts.

AWS has made both types of NZNDB Addendum available online as click-through agreements in AWS Artifact (the customer-facing audit and compliance portal that can be accessed from the AWS management console). In AWS Artifact, customers can review and activate the relevant NZNDB Addendum for those AWS accounts they use to store and process personal information covered by the scheme. NZNDB Addenda frequently asked questions are available online at AWS Artifacts FAQs.

Considerations

This whitepaper does not discuss other New Zealand 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 want to store, where or from whom the content originates, and where the content will be stored.

Customers concerned about their New Zealand privacy regulatory obligations should first ensure they identify and understand the requirements applying to them, and seek appropriate advice.

At AWS, security is always our top priority. We deliver services to millions of 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.

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 AWS Compliance and AWS Cloud Security.

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

- Australia
- California
- Germany
- Hong Kong
- Japan
- Malaysia
- Singapore
- Philippines
- Using AWS in the Context of Common Privacy & Data Protection Considerations

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 AWS security and compliance documents, including the NZNDB Addenda 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, self-paced labs, and instructor-led classes. For more information on AWS training, see AWS Training and Certification.

AWS certifications certify the technical skills and knowledge associated with the best practices for building secure and reliable cloud-based applications using AWS technology. For more information on AWS certifications, see AWS Certification.

If you require further information, please contact AWS or contact your local AWS account representative.

Document revisions

Date	Description
August 17, 2021	Updated for technical accuracy
November 2020	Fifth publication
May 2018	Fourth publication
December 2016	Third publication
January 2016	Second publication
September 2014	First publication

Notes

[1] https://aws.amazon.com/compliance/soc-faqs/

[2] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

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

[4] http://aws.amazon.com/compliance/iso-27017-faqs/

[5] http://aws.amazon.com/compliance/iso-27018-faqs/

[6] https://aws.amazon.com/compliance/iso-9001-faqs/

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

[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) and AWS China (Ningxia) are also isolated AWS Regions. Customers who want to use the AWS China (Beijing) and AWS China (Ningxia) Regions are required to sign up for a separate set of account credentials unique to the China (Beijing) and China (Ningxia) Regions.

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