Using AWS in the Context of South African Privacy Considerations

July 2019

Notices

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

Contents

Abstract

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 in South Africa and the Protection of Personal Information Act, 4 of 2013 (POPIA). 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

Introduction

This document is intended to address the most common questions asked by AWS customers about the potential implications of the POPIA on using AWS services to store or process content containing personal information. There will be other 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.

The information in this document is provided for general informational purposes only, and may not reflect the current law in South Africa. No information contained in this document should be construed as legal advice, nor is it intended to be a substitute for legal counsel on any subject matter. Customers should not act or refrain from acting on the basis of any information presented in this document without seeking the appropriate legal or other professional advice on their specific facts and circumstances that may affect the implementation of privacy and data protection requirements, and more generally, applicable laws relevant to their business.

When we refer to “content” in this document, 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.

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. The AWS shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of privacy requirements that may apply to content that customers choose to store or process using AWS services.

AWS shared responsibility approach to managing cloud security

Will customer content be secure?

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

Security and Compliance is a shared responsibility between AWS and the

customer. This shared model can help relieve customer's operational burden as 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 service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud. The respective roles of the customer and AWS in the shared responsibility model are shown in Figure 1:

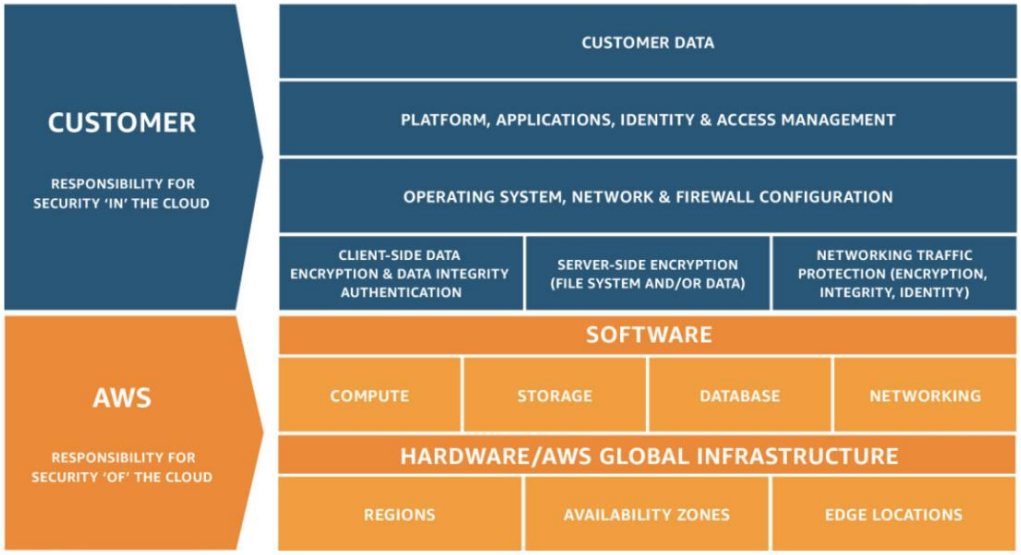

Figure 1 – Shared Responsibility Model

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

AWS responsibility "Security of the Cloud" – AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as

part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

Below are examples of controls that are managed by AWS, AWS Customers and/or both.

Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training – AWS trains AWS employees, but a customer must train their own employees.

Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

AWS Regions: Where can customers store their content

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 have access to twenty-one AWS Regions around the globe[8]. Customers can choose to use one Region, all Regions or any combination of Regions. Figure 2 shows AWS Region locations as at July 2019:

Figure 2 – AWS Global Regions

For a complete list of regions, see the AWS Global Infrastructure page[9].

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 South Africa can choose to deploy their AWS services exclusively in one Region. If the customer makes this choice, their content will be located in that Region unless the customer chooses to move that content or if the content needs to be moved by AWS as necessary to provide the services initiated by the customer or as necessary to comply with the law or a valid and binding order.

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 necessary to provide the services initiated by the customer or as necessary to comply with the law or a valid and binding order.

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.

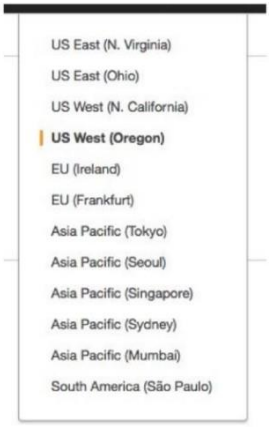

Figure 3 – Selecting AWS Global Regions in the AWS Management Console

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 Ireland region and providing a link (either a VPN[10] or Direct Connect[11]) back to the customer's data centre, all compute resources launched into that VPC would only reside in the Europe (Ireland) Region.

Transfer of personal information across borders

When using AWS services, customers may choose to transfer content containing personal information across borders, and they will need to consider the legal requirements or conditions that apply to such transfers.

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 does not access or use customer content for any purpose other than as legally required and to maintain or provide the AWS services selected by each customer, to that customer and its end users. 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 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 have often misunderstood issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek advice to understand the application of relevant laws to their business and operations.

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

Most countries have legislation that enables law enforcement and government security bodies to seek access to information. However, it is important to remember that these laws all contain criteria that must be satisfied before 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 South African 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 requests from governments unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-U.S. governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services.

Privacy and Data Protection in South Africa The Protection of Personal Information Act, 4 of 2013 (POPIA)

This part of the document discusses aspects of the Protection of Personal Information Act, 4 of 2013 (“POPIA”), which is anticipated to fully come into force in 2019.

One of the primary purposes of POPIA is to establish conditions that regulate the manner in which personal information may be processed. These conditions for the lawful processing of personal information (Conditions) are in line with international standards that prescribe the minimum threshold for the lawful

processing of personal information and encompass accountability, processing limitations, purposes specifications, further processing limitations, information quality, openness, security safeguards and data subject participation.

The Conditions make a distinction between a data controller and a data processor, much like other privacy regimes. The equivalent terms for these parties under POPIA are a responsible party (data controller), the entity that determines the purpose of and means for processing personal information and an operator (data processor), the entity which processes personal information for a responsible party in terms of a contract or mandate. There is an obligation on the responsible party to ensure that its processing of personal information complies with the Conditions. Certain Conditions are also applicable to an operator, albeit to a lesser extent.

As a provider of a self-service infrastructure that is completely under the customers' control – including with respect to how and whether the data is "processed", AWS provides the infrastructure services for customers who want to upload and process content on the AWS network. In this context, AWS does not have any visibility into or knowledge of what customers are uploading onto its network, including whether or not that content includes any personal data. AWS customers are also empowered to use encryption to render content unintelligible for AWS. AWS does not process customer content except as necessary to maintain or provide the services (or to comply with the law or a valid and binding order).

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 that is 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, determines the purpose for which the personal information will be processed, and chooses how the personal information will be processed.
- 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 responsibilities, but the customer, rather than AWS, would manage its relationships with those third parties. For the purposes of this table, we have assumed that the AWS customer will be the responsible party. However, as mentioned above, we acknowledge that there are many circumstances where the AWS customer will be the operator. In these situations, the AWS customer may still find the below useful in the context of its own relationship with the responsible party.

The following table summarises the conditions for the lawful processing of personal information, which a customer should consider if using AWS to store personal information.

Conditions / Requirements	Summary of Condition	Considerations
Accountability	A responsible party must ensure that the conditions for the lawful processing of personal information are complied with, both at the time of determining the purpose and means of processing and during the processing of such information.	**Customer:** The customer collects personal information and determines the purpose of and means for processing such information. It is therefore, incumbent on the customer to ensure that the conditions for the lawful processing of personal information are complied with. **AWS:** To the extent the Conditions 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.

Conditions / Requirements	Summary of Condition	Considerations
Lawfulness of processing	Personal information must be processed lawfully and in a reasonable manner that does not infringe on the privacy of the data subject.	**Customer:** Because the customer collects personal information and determines the purpose of and means for processing such information, there is an obligation on the customer to ensure that personal information is processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject. **AWS:** AWS has no control over what types of content the customer chooses to store in AWS (including whether or not it includes personal data). AWS does not determine what architecture the customer elects to build by combining the AWS service offerings and whether or not it is appropriate for the customer's specific needs. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed. The obligation to ensure that personal information is processed lawfully and in a manner that does not infringe the privacy of the data subject therefore rests on the customer and not AWS.
Minimality	Personal information may only be processed if, given the purposes for which it is processed, it is adequate, relevant and not excessive.	**Customer:** The customer collects personal information and determines the purpose of and means for processing such information. When making this decision, the customer must ensure that the personal information processed is for a legitimate purpose, adequate, relevant and not excessive. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed. The obligation to ensure that personal information is processed adequately, relevantly and not excessively, accordingly rests on the customer and not AWS.

Conditions / Requirements	Summary of Condition	Considerations
Justification	Personal information may only be processed if: (a) the data subject consents[1]; (b) necessary for the conclusion or performance of a contract to which the data subject is a party; (c) the processing complies with applicable laws imposed on a responsible party; (d) the processing protects a legitimate interest of the data subject; (e) the processing is necessary for the proper performance of a public law duty; or (f) the processing is necessary for pursuing the legitimate interest of a responsible party or third party to whom information is supplied.	**Customer:** Because the customer collects personal information and determines the purpose of and means for processing such information, there is an obligation on the customer to ensure that when personal information is processed, the processing of such information is justified. For instance, the customer may process personal information where the data subject has consented to such processing. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed. The obligation to ensure that the processing of personal information is justified accordingly rests on the customer and not AWS.
Collection directly from data subject	Personal information must be collected directly from a data subject unless such collection falls within certain exclusions.	**Customer:** The customer must ensure that personal information is collected directly from the data subject, unless certain exceptions apply, as it is the customer who collects personal information and determines the purpose of and means for processing such information. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed, and has no control over what information is collected or the purposes of such collection. Accordingly, the obligation to collect personal information directly from the data subject rests with the customer.

[1] Where the data subject is a child (a person under the age of 18 years), consent is required from the person who is legally competent to provide consent on behalf of the child.

Conditions / Requirements	Summary of Condition	Considerations
Collection for specific purposes	Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.	**Customer**: The customer, as the responsible party, must ensure that personal information is collected for a specific, explicitly defined and lawful purpose. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed, and has no control over what information is collected or the purposes of such collection. Accordingly, this obligation rests on the customer.
Retention and restriction of records	Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless such retention falls within certain exclusions. The responsible party must destroy or delete personal information as soon as reasonably practicable after it is no longer authorised to retain the personal information. The destruction or deletion of such information must be done in a manner that prevents its reconstruction in an intelligible form. In certain circumstances, the responsible party must also restrict the processing of information.	**Customer:** The customer, as the responsible party, must ensure that records of personal information are not retained for any longer than necessary and access is restricted. **AWS:** AWS has no insight into whether stored data includes personal information or to the purposes for which the customer is processing any particular data which it has stored in the AWS cloud. Accordingly, it cannot determine for how long it is necessary to retain the data in order to achieve that purpose. When a customer deletes its content from the AWS services, the content is rendered unreadable or disabled and the underlying storage areas on the AWS network that were used to store the content are wiped, prior to being reclaimed and overwritten, in accordance with AWS standard policies and deletion timelines. AWS procedures also include a secure decommissioning process conducted prior to disposal of storage media used to provide the AWS services. As part of that process, storage media is degaussed or erased and physically destroyed or disabled in accordance with industry standard practices.

Conditions / Requirements	Summary of Condition	Considerations
Further processing limitation	Further processing of personal information must be in accordance or compatible with the purpose for which it was originally collected.	**Customer:** The customer, as a responsible party, must ensure that any further processing of personal information is in line with the purposes for which the information was originally collected. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed, and has no control over what information is collected or the purposes of such collection. Accordingly, this obligation rests on the customer.
Information quality	A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and up to date.	**Customer:** It is the responsibility of the customer to ensure that personal information processed is complete, accurate, not misleading and up to date. The customer has control over the personal data which it chooses to store on AWS. It is therefore responsible for verifying and maintaining its accuracy (and can update and correct it as necessary). In addition, the customer manages and is responsible for the security 'in' the cloud, and so the customer is able to ensure that it has implemented appropriate measures to protect against corruption of the data. **AWS:** AWS has no control over what types of content the customer chooses to store in AWS, and no insight into this content. AWS does not enter or modify any data on the customer's behalf. It is therefore unable to verify the accuracy of this data or update it. However, SOC 1 Type 2 report includes details of the controls that AWS maintains to ensure the integrity of the data at the level of the underlying cloud environment.

Conditions / Requirements	Summary of Condition	Considerations
Openness	Where personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of various aspects. In particular, the responsible party must ensure that the data subject is aware that the responsible party intends to transfer the information to a third country or international organization, and the level of protection afforded in such circumstances.	**Customer:** There is an obligation on the customer, as a responsible party, to ensure that when personal information is collected, the data subject is aware of such collection. The customer must ensure that where it elects to store personal information on the AWS cloud in Regions outside of the Republic of South Africa, it ensures that this is brought to the attention of the data subject. **AWS:** AWS simply provides the infrastructure services for customers who want to upload and process content on the AWS network and has no control over what information is collected or the purposes of such collection. Accordingly, this obligation rests on the customer.
Transfer of personal information outside Republic of South Africa (RSA)	A responsible party in the RSA may not transfer personal information concerning a data subject to a third party who is in a foreign country unless: (a) the third party is subject to law, binding corporate rules or binding agreements which provide for an adequate level of protection; (b) the data subject consents; (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party; (d) the transfer is necessary for the performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or (e) the transfer is for the benefit of data subject and in circumstances where it is not reasonably practicable to obtain consent and if it were, the data subject would provide consent.	**Customer:** There is an obligation on the customer, as the responsible party, to ensure that when personal information is transferred outside RSA, certain criteria are satisfied. For instance, when the customer chooses to store information in a Region outside of the RSA, consent is received from the data subject. **AWS:** AWS does not move customer content outside of the customer's chosen Region(s) except as necessary to provide the services initiated by the customer or to comply with the law or a valid and binding order. AWS provides a data processing addendum to help customers meet their data protection obligations.

Conditions / Requirements	Summary of Condition	Considerations
Security safeguards	A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking certain measures to prevent loss of, damage to, unauthorized destruction of and unlawful access or processing of to personal information. Anyone who processes personal information on behalf of a responsible party must (a) process such information only with the knowledge or authorization of the responsible party and (b) treat personal information which comes to their knowledge as confidential. It is the responsibility of the responsible party to ensure that an operator who processes information on its behalf, maintains certain security measures. Where there are reasonable grounds to believe that personal information has been accessed or acquired by unauthorized means, the operator must immediately notify the responsible party.	**Customer:** The customer, as a responsible party, must ensure the integrity and confidentiality of personal information by taking certain measures to prevent loss of, damage to, unauthorized destruction of and unlawful access to personal information. In line with this, customers are responsible for security in the cloud, including security of their content and implementing an appropriate architecture using the AWS service offerings. In particular, customers are responsible for properly (a) configuring the AWS services, (b) using the controls available in connection with the services, and (c) taking such steps as they consider necessary to maintain appropriate security controls and backup of their personal data (e.g. by using encryption technology to protect the personal data from unauthorized access, and routine archiving). **AWS:** AWS maintains certain security measures, and in line with this, is responsible for managing the security of the underlying cloud environment. AWS uses external auditors to verify the efficacy of its security measures, including the security of the physical data centres from which AWS provides its services. AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Conditions / Requirements	Summary of Condition	Considerations
Data subject participation	A data subject has the right to request a responsible party to confirm whether it holds personal information of the data subject and request for a copy of the record of personal information held by the responsible party. In addition, a data subject has the right to request that the responsible party correct, delete or destroy personal information.	**Customers:** The customer retains control of content stored on AWS, and therefore, can decide how data subjects may access any of their personal data included in that content. Similarly, it is the customer who is best placed to be able to respond to a request or complaint from a data subject regarding the lawfulness of the customer's data processing activities. **AWS:** As explained above, AWS has no control over what types of content the customer chooses to store in AWS and for what purposes. AWS has no insight into this content (including whether or not it includes personal data). AWS cannot identify and has no contact with data subjects whose personal data the customer has chosen to store in AWS (except in cases where this relates to the customer him/herself), and is therefore not able provide any information to the relevant data subjects. AWS has no ability to connect data stored on AWS with any particular person. That information is exclusively in the customers' control.
Processing of special personal information and personal information of children.	A responsible party may only process special personal information in certain circumstances. Special personal information includes: religious or philosophical beliefs; race or ethnicity; trade union membership; political persuasion; health, sex life or biometric information; and the criminal behavior of a data subject. A responsible party may only process personal information of children in certain circumstances.	**Customer:** Since it is the customer who collects personal information and determines the purpose of and means for processing such information, there is an obligation on the customer to ensure that when it processes special personal information or personal information of children, the processing of such information is not unlawful. **AWS:** AWS has no control over the purposes for which the customer uses its content and stores it in the AWS cloud. AWS plays no role in the decision-making as to whether and for what purposes this data will be processed, and has no control over what information is collected or the purposes of such collection. Accordingly, this obligation rests on the customer.

Other considerations

This document does not discuss other South African privacy laws, aside from the provisions of the POPIA, which 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 South African 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.

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 (https://do.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf)
- European Union (https://do.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf)
- Malaysia

(https://do.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf)

- New Zealand (http://do.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf)
- Singapore (https://do.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf)

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS cloud and gain proficiency with AWS services and solutions. We offer free instructional videos, self-paced labs, and instructor-led classes. Further information on AWS training is available at http://aws.amazon.com/training/.

AWS certifications certify the technical skills and knowledge associated with best practices for building secure and reliable cloud-based applications using AWS technology. Further information on AWS certifications is available at http://aws.amazon.com/certification/.

If you require further information, please contact AWS at: https://aws.amazon.com/contact-us/ or contact your local AWS account representative.

Notes

[1] https://do.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper. pdf

[2] http://aws.amazon.com/compliance/soc-faqs/

[3] http://do.awsstatic.com/whitepapers/compliance/soc3 amazon web services.pdf

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

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

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

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

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

[9] https://aws.amazon.com/about-aws/global-infrastructure/

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

[11] http://aws.amazon.com/directconnect/

[12] https://aws.amazon.com/compliance/eu-data-protection/

Document Revisions

Date	Description
November 2017	First Publication.
July 2019	Second Publication.