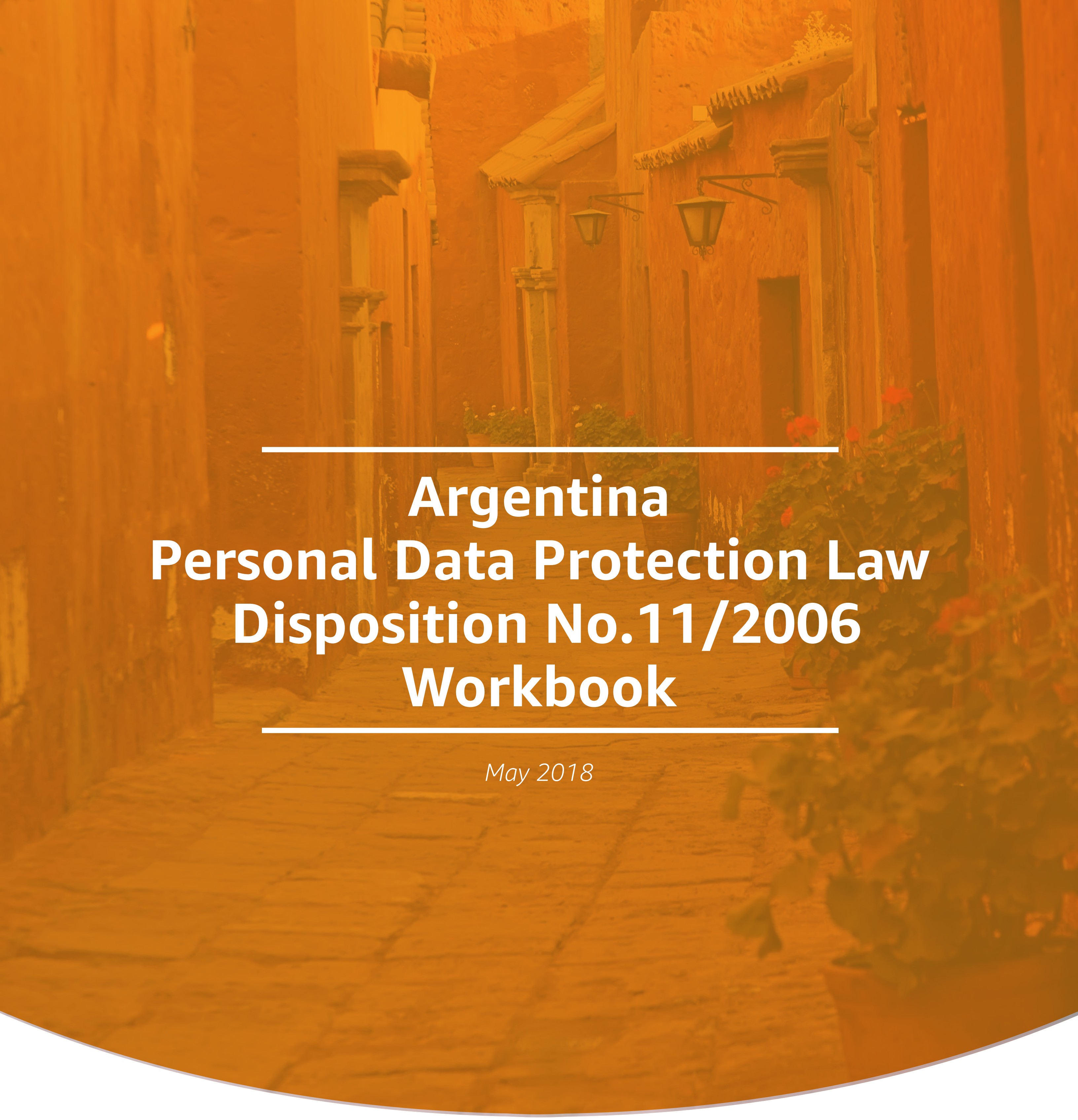


Argentina
Personal Data Protection Law
Disposition No.11/2006
Workbook

May 2018

[Workbook]

Notices

This document is provided for informational purposes only. It represents AWS' 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' 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 data, in the context of Argentina's Personal Data Protection Law No. 25,326, including Regulatory Decree No. 1558/2001 and supplementary regulations ("PDPL"), that applies to the protection of personal data in Argentina and when personal data is transferred internationally for processing.

The Argentine Data Protection Authority enacted Disposition No. 11/2006 under the PDPL, which describes three different levels of technical and organizational security measures (basic, medium and critical) to consider depending on the activities you conduct or the nature of the personal data that you process.

This workbook will help customers to implement the controls listed in Disposition No. 11/2006 – Addendum I.

Scope

This workbook focuses on typical questions asked by AWS customers when they are considering privacy and data protection requirements relevant to their use of AWS services to store or process content containing personal data. There will also be other relevant considerations for each customer to address, for example, a customer may need to comply with industry specific requirements, the laws of jurisdictions where that customer conducts business or contractual commitments a customer makes to a third party.

This document 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.

For more information, please visit https://aws.amazon.com/compliance/argentina-data-privacy/.

Considerations relevant to privacy and data protection

When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

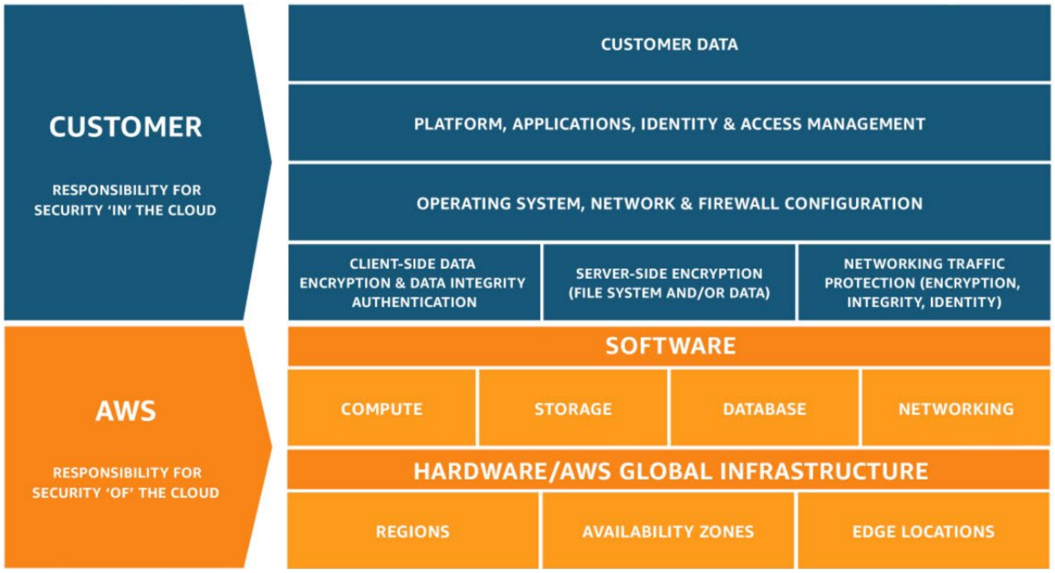
- What content they choose to store or process using AWS services
- Which AWS services they use with their content
- The Region(s) where their content is stored
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted
- Who has access to their AWS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

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

For complementary information about how AWS services operate, including how customers can address security and encrypt their content, the geographic locations where customers can choose to store content, and for other relevant considerations, please access the whitepaper Using AWS in the Context of Common Privacy & Data Protection Considerations.

Security and Shared Responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data center.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Shared Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

Security in the Cloud

Customers are responsible for their security in the cloud. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and 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 they use, the integration of those services into their IT environments, and applicable laws and regulations.

It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customers are responsible for the 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.

Security of the Cloud

In order to provide Security of the Cloud, AWS continuously audits its environments. The infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that can be implemented, and to better assist customers with managing their control environment.
- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitor**, through the use of thousands of security control requirements, that AWS maintains compliance with global standards and best practices.

AWS Compliance Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads, including the following:

ISO 27001 – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

ISO 27017 – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

ISO 27018 – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

ISO 9001 - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

PCI DSS Level 1 - The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

SOC – AWS System & Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:

- **SOC 1:** Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
- **SOC 3:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see the AWS Assurance Programs webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes whitepaper.

Argentina - Personal Data Protection Law - Disposition No. 11/2006

Disposition No. 11/2006 – Addendum I prescribes the security measures applicable to the treatment and conservation of personal data contained in archives, records, and public non-State and private databases. http://www.jus.gob.ar/media/33445/disp_2006_11.pdf

This section of the document provides information relating to each control listed in Disposition No. 11/2006, who has responsibility for controls compliance within the AWS Shared Security Model and, in cases where AWS shares responsibility, how customers can use AWS Cloud Compliance resources to evidence their compliance to particular controls.

No.	Requirement	Responsibility	Considerations
BASIC LEVEL SECURITY MEASURES Databases containing personal data shall adopt the following security measures which are classified as Basic Level as detailed below: Implement a “Security Manual” for personal data specifying, among other requirements, the proceedings and security measures applicable to databases and files containing personal data. The Security Manual must be updated periodically and revised when changes are made to the information system. It must contain the following:			
1	Responsibilities and obligations of staff.	Customer	Customers new to cloud computing can review an overview of the AWS Cloud Adoption Framework which helps organizations develop efficient and effective plans for their cloud adoption journey. Additional information can be found on website at https://aws.amazon.com/professional-services/CAF/. New customers are also welcomed to read more about security processes on Intro to Security Processes, which references, but is not limited to, the Shared Responsibility Model, Physical and Environmental Security, Business Continuity, Design Principles and Security Features.
2	Description of databases and information systems that process the personal data.	Customer	Customers retain control and are responsible for their data, security controls and procedures.

No.	Requirement	Responsibility	Considerations
3	Description of data control routines of the programs that collect data and the actions to follow in case of errors to correct them. All programs that collect data must include, regardless of the means of processing (including batch or interactive), control routines that minimize the risk of incorporating illogic, incorrect or missing data into the information system.	Customer	Customers retain control and are responsible for their data, security controls and procedures.
4	Registry of security incidents. Notification, management and responses to security incidents.	Shared	Customers can maintain a variety of logs and automate notifications. AWS offers services such as Amazon CloudWatch to monitor AWS cloud resources and the applications you run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, send notifications, and automatically react to changes in your AWS resources. With AWS CloudTrail, you can log, continuously monitor, and retain events related to application programming interface (API) calls across your AWS infrastructure. For more information on logging & monitoring visit, http://aws.amazon.com/whitepapers/aws-security- best-practices/. AWS has implemented a formal, documented incident response policy and program developed in alignment with ISO 27001 standards. The system utilities are appropriately restricted and monitored. AWS SOC reports provide additional details on controls in place to restrict system access. For more information, please refer to the Incident Response section on the AWS: Overview of Security Processes whitepaper at https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.
5	Back-up procedures and data recovery.	Customer	AWS allows customers to perform their own backups by using services like Amazon Simple Storage Service and Amazon Glacier, which are designed to deliver 99.999999999% durability. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://aws.amazon.com/whitepapers/backup-and-recovery-using-aws/.

No.	Requirement	Responsibility	Considerations
6	An updated access control listing.	Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers an easy way to list users, groups, roles and policies that enables data access directly from AWS management console. Security and user management using IAM are carefully explained in the AWS Security Best Practices whitepaper (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), on Manage AWS Accounts, IAM Users, Groups, and Roles section.
7	Procedures to identify and authenticate users of data authorized to use certain information systems. Access control lists shall be kept up to date. A password policy shall apply to systems that require passwords for authentication. The password policy requires that passwords are set by the person responsible for the security of the account through a process that guarantees confidentiality, passwords are changed periodically (within a maximum term), and stored passwords are encrypted or hashed.	Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. Customers can use AWS APIs to configure access control permissions for any of the services they develop or deploy in an AWS environment. AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on our website at https://aws.amazon.com/iam/. Strategies for managing users, groups, roles and granting access to customer data can be found on the AWS Security Best Practices whitepaper (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), under Manage AWS Accounts, IAM Users, Groups, and Roles section.
8	Users' access to systems shall be provisioned based on the principle of least privilege.	Shared	Customers maintain full control and responsibility for configuring access to their data. AWS employs the principle of least privilege, allowing only the necessary access for users to accomplish their job function. New user accounts are created to have minimal access. User access to AWS systems (for example, network, applications, tools, etc.) requires documented approval from the authorized personnel (for example, user's manager and/or system owner) and validation of the active user in the HR system. Information Security Management Systems (ISMS) should be defined and utilized. More information on designing your ISMS to protect your assets on AWS can be found on the AWS Security Best Practices whitepaper (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), under the section with the same name.

No.	Requirement	Responsibility	Considerations
9	Updated anti-virus, malware, or advanced threat protection software shall be installed on end-points to scan for, detect and eliminate viruses. Before using any documents received through a website, e-mail or any other unknown origin, you must verify that they do not contain any virus.	Customer	Customers retain control and are responsible for their data, security controls and procedures.
10	Procedures that guarantee the adequate management of the information systems that store or process personal data (identification of the type of information, storage at places of restricted access, inventories, authorization to remove data from premises, destruction of obsolete data, etc.). Note: If the databases include personal data that, if treated in a certain way, would allow someone to determine the identity or conduct of an individual, then the measures listed in Sections 2, 3, 4 and 5 under the Medium Level security measures shall be also put in place.	Shared	Procedures and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and access to customer data is appropriately segregated from other customers. All content and data is classified according to the requirements of the Amazon Data Classification Policy. Data classified as Critical is AWS's most sensitive data. All data is handled according to the Data Handling Standard and Data Retention Policy. AWS classifies all media entering AWS facilities as Critical and treats it accordingly as high impact throughout its life-cycle. AWS classifies all customer content and associated assets as Critical. Customer information is not used in test and development environments. Additional information on these procedures and mechanisms can be found on the AWS: Overview of Security Processes whitepaper https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

No.	Requirement	Responsibility	Considerations
MEDIUM LEVEL SECURITY MEASURES The databases and files from private entities developing public service activities, as well as databases and files belonging to entities performing a public and/or private activity that, notwithstanding the section 10 of the Law No. 25,326, must keep information in secret as per an express legal obligation (i.e. bank secrecy), shall implement the following security measures, in addition to those applicable to the Basic Level:			
1	The Security Manual must identify a person (or specific unit) responsible for the security.	Customer	Customers retain control and are responsible for their data, security controls and procedures. Customers new to cloud computing can review an overview of the AWS Cloud Adoption Framework which helps organizations develop efficient and effective plans for their cloud adoption journey. Additional information can be found on our website at https://aws.amazon.com/professional-services/CAF/.
2	Perform internal or external audits to verify compliance with security measures related to personal data. The audit reports must be submitted to the owner of the database in order to implement any necessary corrective measures. When the Argentine Personal Data Protection Authority performs an inspection it must consider, on a non-binding basis, the results of the aforementioned audits, provided that such audit has been performed within the last year.	Shared	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements SSAE 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications. For more information on AWS compliance reports, please visit https://aws.amazon.com/compliance/.

No.	Requirement	Responsibility	Considerations
3	Limit the possibility of repeated attempts of unauthorized access to information systems.	Customer	Customers retain the control and responsibility of their data and associated media assets. Customer can define their Password Policy in AWS environment: For more details, see Setting an Account Password Policy for IAM Users at http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html .
4	Physical access controls must be put in place in the premises where personal data is stored.	Shared	Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to perform their jobs. Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and ensure that only authorized individuals enter an AWS data center. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. Trained security guards are stationed at the building entrance 24x7x365. If a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. Learn more about how we secure AWS data centers by design by taking a virtual tour at https://aws.amazon.com/compliance/data-center/. Additional information on physical and environmental security can be found in the AWS: Overview of Security Processes whitepaper (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) under the section with the same name.

No.	Requirement	Responsibility	Considerations
5	Database and information management. Registry of accesses and exits of information from the databases detailing date and time of each activity, the receiving and issuing parties, the method of transmission, among others. Implementing the necessary measures to prevent the recovery of data from a database or device after it is destroyed or recycled. Furthermore, similar measures shall be adopted when the information or the devices exit the facilities in which they are located (e.g., when making backup copies, the information travels from a local support system to another remote site). Recovery and processing backup data procedure shall be implemented, in case of contingencies which may render the customary processing equipment nonoperative.	Shared	AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. See the AWS Cloud Security whitepaper for additional details - available at https://d0.awsstatic.com/whitepapers/Security/ES_Whitepapers/AWS_Security_Whitepaper.pdf. On the customer side, as stated in the Shared Responsibility Model, customers are responsible for putting data protection and backups in place by using its own software or using one or more services offered by AWS. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS at https://aws.amazon.com/whitepapers/backup-and-recovery-using-aws/. Customers are also responsible for managing the lifecycle of their data, and purging and auditing whenever necessary or needed.
6	In case of a data recovery, the registry of security incidents must identify the individual who recovered or modified the data. A written authorization from the owner of the database is also required.	Shared	AWS has implemented a formal, documented incident response policy and program developed in alignment with ISO 27001 standards. The system utilities are appropriately restricted and monitored. AWS SOC reports provides additional details on controls in place to restrict system access. AWS offers services such as Amazon CloudWatch to monitor AWS cloud resources and the applications you run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, send notifications, and automatically react to changes in your AWS resources. With AWS CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. For more information on logging & monitoring visit http://aws.amazon.com/whitepapers/aws-security- best-practices/.

<table>
<tr><th>No.</th><th>Requirement</th><th>Responsibility</th><th>Considerations</th></tr>
<tr><td>7</td><td>Service tests undertaken prior to the launch of new information systems shall not be conducted with personal data, unless the appropriate levels of security corresponding to the nature of the personal data have already been put into place.</td><td>Customer</td><td>Customers retain control and are responsible for their data, security controls and procedures.</td></tr>
<tr><td colspan="4"><u>CRITICAL LEVEL SECURITY MEASURES</u>
In addition to the security measures applicable to Basic and Medium Levels, databases and files containing “sensitive data” (with certain exceptions detailed below) must implement the following additional measures:
Note: databases that must process sensitive data for administrative purposes or to comply with legal obligations shall be excluded from implementing these critical level security measures. Nevertheless, adequate and necessary security measures must be implemented pursuant to the type of data to be processed.</td></tr>
<tr><td>1</td><td>When personal data is being transported in equipment — including the back-up copies - it must be encrypted (or any other similar measure) in order to guarantee that it is not readable or able to be manipulated while in transit.</td><td>Customer</td><td>AWS offers you the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. This includes:
• Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift.
• Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys.
• Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements.
In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.</td></tr>
</table>

No.	Requirement	Responsibility	Considerations
2	An access registry must include information that identifies users, when they log in (including date and time), type of access and if access has been granted or denied. In cases where access has been granted, the registry shall also identify the information accessed and the actions performed by such user (e.g., amendment, deletion, etc.). This registry shall be periodically reviewed by the person responsible for security and shall be kept for at least 3 years.	Customer	Customers retain control and are responsible for their data, security controls and procedures. Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. For additional details visit https://aws.amazon.com/cloudtrail/. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. For additional details visit https://aws.amazon.com/cloudwatch/. AWS provide customers with the ability to delete their data. However, AWS customers retain control and ownership of their data so it is the customer's responsibility to manage data retention in accordance with their own requirements.
3	In addition to the backup data that is kept in the data facility, back-up data must also be maintained in an external data facility located at a prudent distance from the other data facility, and must be kept in fireproof boxes or in safe deposit boxes. There must be a recovery procedure and a contingency plan in place in the event that the customary processing equipment becomes non-operational.	Customer	Each customer has the responsibility to enable or design the correct architecture for its resources to meet this requirement (Whether multi-availability zone or multi-region). Customers can choose to back up their data in any one Region, all Regions or any combination of Regions, including Regions in Brazil and the United States. Visit the AWS Global Infrastructure website for a complete list of AWS Regions.

No.	Requirement	Responsibility	Considerations
4	Personal data that is transferred though network communications* must be encrypted or using a similar measure in order to guarantee that it is not readable or able to be manipulated by unauthorized individuals. **Refers to communications that exit the network of the organization.*	Customer	AWS offers you the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. This includes: • Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift. • Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys. • Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements. In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

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.

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. These resources can be found at http://aws.amazon.com/compliance and http://aws.amazon.com/security.

Document Revisions

Date	Description
May 2018	First publication.