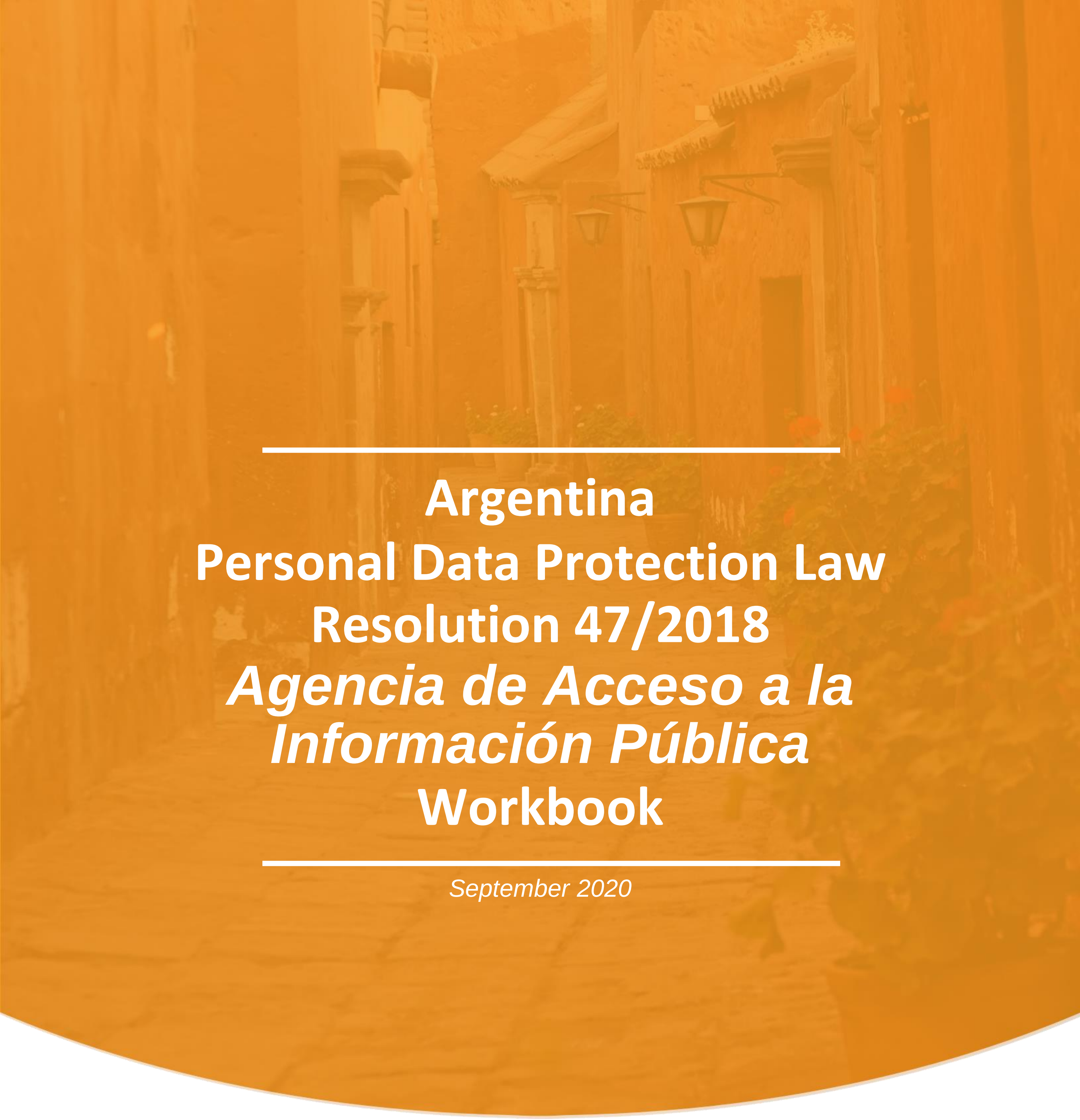


Argentina
Personal Data Protection Law
Resolution 47/2018
Agencia de Acceso a la Información Pública
Workbook

September 2020

[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.

In July 2018, the Argentine Data Protection Authority (*Agencia de Acceso a la Información Pública*, or "Authority") issued Resolution 47/2018 under the PDPL, which repealed Disposition No. 11/2006 and approved new, recommended security measures aligned with international best practices and standards and aimed to protect the confidentiality and integrity of personal data during its processing – from data collection to data deletion.

This workbook will:

- help customers understand the respective roles that the customer and AWS each play in managing and securing the cloud environment
- provide an overview of the recommended security measures listed in Resolution 47/2018 – Annex I (*Medidas de seguridad recomendadas para el tratamamiento y conservación de los Datos Personales en medios informatizados*), and
- provide additional considerations on how customers can implement any applicable security measures when using AWS services.

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 regarding the Argentina data privacy framework and other relevant privacy and data protection considerations AWS customers should consider, 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

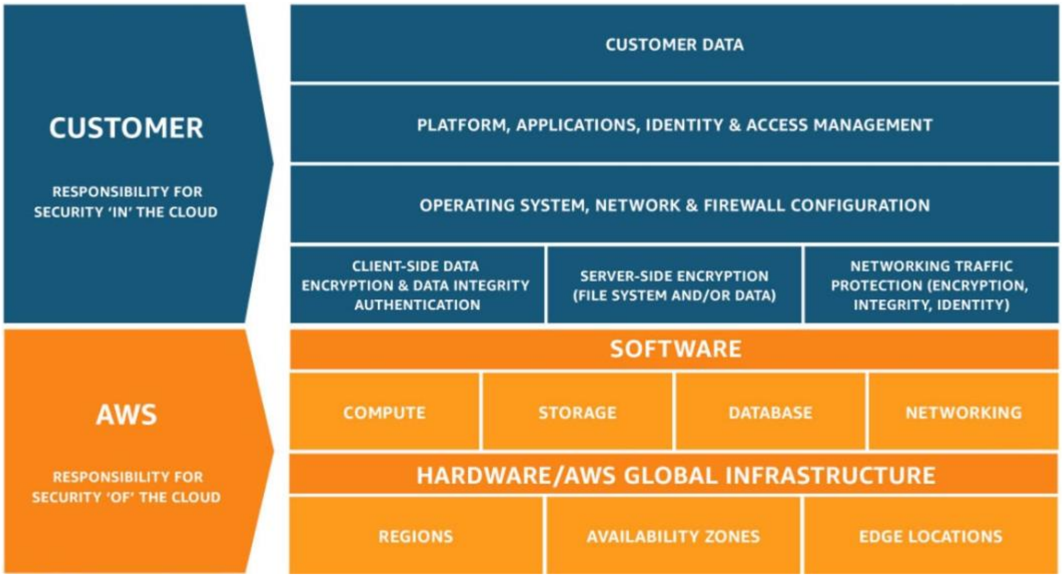
Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model.

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.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. 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).

Argentina - Personal Data Protection Law - Resolution 47/2018

September 2018, the Authority issued Resolution 47/2018 ("Resolution 47") under the PDPL, which repealed Disposition No. 11/2006 related to security measures that data controllers (i.e., AWS customers) needed to consider when processing personal data.

Resolution 47 describes new, recommended security measures aligned with international best practices and standards, and aimed to protect the confidentiality and integrity of personal data during its processing – from data collection to data deletion. In particular, this new resolution updated the list of measures and controls recommended to manage, plan, control, and improve the security when processing personal data. These recommended security measures are divided by processing related activities, including data collection, access controls, change controls, backup and recovery, vulnerability management, data removal or deletion, security incidents and development environments.

In accordance with Section 9 of the PDPL, a "data controller" (i.e., *responsable o usuario de datos*) must adopt technical and organization measures to guarantee the security and confidentiality of personal data and avoid its alteration, loss, unauthorized access or processing. Through Resolution 47, the Authority has provided additional guidance and a list of **recommended** security measures for you to consider when processing personal data using AWS.

The tables below list each of the recommended security measures included in Resolution 47 (Annex I – *Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados*), and provide additional considerations on how AWS customers can implement any applicable security measures when using AWS services. These tables contain only a non-exhaustive sample of considerations. This is not legal or compliance advice, customers should consult with their own legal and compliance teams.

No.	Recommended Security Measures[1][2]	Responsibility	AWS Considerations
A. DATA COLLECTION Related to the procedures necessary to ensure the completeness and integrity of data, minimize mistakes and implement technical measures to warrant confidentiality and limit access during the collection process.			
A.1 Integrity	A.1.1 To ensure data completeness A.1.2 To minimize uploading mistakes A.1.3 To ensure data integrity	Customer	The customer determines and controls when, how and why it collects personal data from individuals, and decides whether it will include that personal data in customer content it stores or processes using the AWS services. The customer may also need to ensure it discloses the purposes for which it collects that data to the relevant data subjects, obtains the data from a permitted source and that it only uses the data for a permitted purpose. AWS customers are responsible for implementing mechanisms to protect the confidentiality and integrity of collected, transmitted, shared, stored, or otherwise processed customer content when using AWS services. Therefore, in the context of customer content stored or processed using the AWS services, the customer:

[1] *Personal Data* refers to the "information of any kind related to determined or determinable individuals or legal entities" and *Sensitive Data* refers to "personal data revealing racial and ethnic origin, political opinions, religion, philosophical or moral beliefs, membership to an union association, health data and information on sexual orientation" as defined in the section 2 of the Personal Data Protection Law No. 25.326.

[2] These tables list the recommended security measures for "personal data," unless otherwise expressly indicated that they relate to "sensitive data".

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			□ Collects personal data from its end users or other individuals (data subjects), and determines the purpose for which the customer requires and will use the personal data □ Has the capacity to control who can access, update and use the personal data □ Manages the relationship with the individual about whom the personal data relates (referred to as a data subject), including by communicating with the data subject as required to comply with any relevant disclosure and consent requirements. As such, the customer performs the role of a data controller, as it controls its content and makes decisions about treatment of that content, including who is authorized to process that content on its behalf. By comparison AWS performs a role of a data processor, as AWS only uses customer content to provide the AWS services selected by each customer and does not use customer content for other purposes. 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 our whitepaper Amazon Web Services: Overview of Security Processes, which references, but is not limited to, the Shared Responsibility Model, Physical and Environmental Security, Business Continuity, Secure Design Principles and Security Features.
A.2 Confidentiality	A.2.1 To warrant confidentiality during the entire data collection process	Customer	The customer determines and controls the reason it collects personal data, what it will be used for, who it can be used by and who it is disclosed to. AWS provides HTTPS endpoints using the TLS (Transport Layer Security) protocol for communication, which provides encryption in transit when you use AWS APIs (Application programming interface). You can use the AWS Certificate Manager (ACM) service to generate, manage, and deploy the private and public certificates you use to establish encrypted transport between systems for your workloads. Amazon Elastic Load Balancing is integrated with ACM and is used to support HTTPS protocols.
	A.2.2 To restrict access to data collection A.2.3 To limit unauthorized access during data collection	Customer	While under the Shared Responsibility Model, access control for customer content 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, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
	A.2.3 To limit unauthorized access during data collection **Sensitive Data**	Customer	Under the Shared Responsibility Model, access control for customer data is a customer responsibility. AWS provides HTTPS endpoints using the TLS (Transport Layer Security) protocol for communication, which provides encryption in transit when you use AWS APIs. You can use the AWS Certificate Manager (ACM) service to generate, manage, and deploy the private and public certificates you use to

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			establish encrypted transport between systems for your workloads. Amazon Elastic Load Balancing is integrated with ACM and is used to support HTTPS protocols. If your content is distributed through Amazon CloudFront, it supports encrypted endpoints.
B. ACCESS CONTROL Related to the implementation of security measures, authentication mechanisms, classification of roles and tasks, and further features of the access to systems designed to protect identity and privacy.			
B.1 Identification of assets	B.1.1 Identify assets	Customer	AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their IT assets hosted in AWS. AWS customers are responsible for verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability. Customers can use AWS Config to access to a detailed view of the configuration of the AWS resources in their AWS account. This includes how the resources are related to one another, and how they were previously configured, so that they can see how the configurations and relationships change over time With AWS Config, customers are able to continuously monitor and record configuration changes of their AWS resources. AWS Config also enables customers to inventory their AWS resources, the configurations of their AWS resources, as well as software configurations within EC2 instances at any point in time.
	B.1.2 Identify responsible parties and determine their responsibilities		
	B.1.3 Verify the controls application		
B.2 Access of Data	B.2.1 Manage access to systems	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. Also IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are carefully explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
	B.2.2 Assign permissions	Shared	AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing an access control policy and supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization. AWS implements formal, documented policies and procedures in alignment with ISO 27001 standards that provide guidance for operations and information security within the organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities, and management commitment. All policies are maintained in a centralized location that is accessible by AWS employees. Customers can validate these policies, procedures and controls implemented at the organization level in our AWS' security and compliance reports available in AWS Artifact.

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It 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.
	B.2.3 Verify the identification and the authorization	Shared	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, on Manage AWS Accounts, IAM Users, Groups, and Roles section. Customers retain the control and responsibility of their data and associated media assets. Customer can define their "Password Policy" on their AWS account to specify complexity requirements and mandatory rotation periods for their IAM users' passwords. For more details, see Setting an Account Password Policy for IAM Users were you will learn how to set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. AWS controls access to AWS systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.
	B.2.4 Control physical access to data centers	AWS	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 under the section with the same name.

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System & Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI DSS compliance reports.
	B.2.5 Monitor the activity	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, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
	B.2.5 Monitor the activity **Sensitive Data**	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. Also our customers can use AWS CloudTrail to monitor their account activity. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts Security and user management using IAM are carefully explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
C. CHANGE CONTROL Related to the implementation of procedures for the effective identification of any person that accesses productive environments containing personal data to introduce changes, ensuring his/her identification, authentication and relevant authorization.			
C1. Change Control	C.1.1 Ensure changes	Customer	Customers retain control of content stored or processed using AWS, including control over how that content is secured and who can access and amend that content. 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 and monitoring visit, https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/
	C.1.1 Ensure changes **Sensitive Data**	Customer	AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing an access control policy and supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization.

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
D. BACKUP AND RECOVERY Designed to implement backup processes that may allow an adequate recovery of the data in the event of an incident that prevents access to data originally stored, and define data security practices, data disclosure, and training, for the development of preventive and remedial tasks related to security incidents.			
D.1 Backup copies and recovery procedure	D.1.1 Ensure a formal backup and recovery procedure	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. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway. Using AWS Backup, customers can centrally configure backup policies and monitor backup activity for AWS resources, such as Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon EFS file systems, and AWS Storage Gateway volumes. AWS Backup automates and consolidates backup tasks previously performed service-by-service, removing the need to create custom scripts and manual processes. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, enabling you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
	D.1.2 Ensure access control	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. 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://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), under Manage AWS Accounts, IAM Users, Groups, and Roles section.
	D.1.2 Ensure access control **Sensitive Data**	Shared	AWS Customers should architect their AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS' infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier -1 transit providers. For additional information, please see AWS Global Infrastructure website available at https://aws.amazon.com/about-aws/global-infrastructure/.
E. VULNERABILITY MANAGEMENT Related to the implementation of ongoing review procedures that allow to identify, analyze, evaluate and correct all possible vulnerabilities of IT-based data systems by applying control techniques related to integrity, registry, traceability and verification.			
E.1 Vulnerabilities Management	E.1.1 Prevent security incidents by design	Shared	Customers retain control and are responsible for their data, security controls and procedures. 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. In addition, customers can use our Security by Design (SbD) whitepaper, which discusses the concepts of Security by Design, provides a four-phase approach for security and compliance at scale across multiple industries, points to the resources available to AWS customers to implement security into the AWS environment, and describes how to validate controls are operating.
	E.1.2 Ensure proper protection	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 our website at https://aws.amazon.com/professional-services/CAF/.
	E.1.3 Detect possible security incidents	Shared	Customers retain control and are responsible for their data, security controls and procedures. 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, https://aws.amazon.com/whitepapers/aws-security-best-practices/. Also, customers can use Amazon GuardDuty to protect their AWS accounts and workloads with

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			intelligent threat detection and continuous monitoring. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect their AWS accounts and workloads. 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.
	E.1.2 Ensure proper protection **Sensitive Data**	Customer	Customers retain control and are responsible for their data, security controls and procedures. Customers can use AWS WAF, a web application firewall, to address the top application security flaws as named by the Open Web Application Security Project (OWASP). Using AWS WAF, you can write rules to match patterns of exploitation attempts in HTTP/S requests and block requests from reaching your web servers. For more information, please refer to the “Use AWS WAF to Mitigate OWASP’s Top 10 Web Application Vulnerabilities” whitepaper: https://d1.awsstatic.com/whitepapers/Security/aws-waf-owasp.pdf
	E.1.4 Ensure efficient and lasting measures **Sensitive Data**	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/.
F. DATA DELETION Related to the implementation of data deletion procedures, to confirm that confidential data is duly deleted by using safe deletion methods and applying an efficient control of the deletion procedure.			

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
F1. Data Deletion	F.1.1 Establish a data deletion process	Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymize the personal data when no longer needed. For more information on Data Lifecycle, please review our "[Using AWS in the context of common privacy and data protection considerations]" whitepaper The AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation (https://aws.amazon.com/documentation/).
	F.1.2 Establish secure deletion methods	Shared	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. The AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation (https://aws.amazon.com/documentation/). In alignment with ISO 27001 standards, when an AWS 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.
	F.1.3 Appoint a responsible person for data deletion	Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures.
	F.1.4 Monitor the deletion process		
	F.1.2 Discard of media devices **Sensitive Data**	Shared	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures, including the implementation of secure deletion methods or techniques. The AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation (https://aws.amazon.com/documentation/). Regarding AWS storage media devices: Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycle. We have standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.
G. SECURITY INCIDENTS Related to the management of security incidents that may affect personal data, and their detection, evaluation, processing and response, as well as reporting and corrective measures.			
G.1 Notification of security incidents	G.1.1 Define responsibilities and procedures	Customer	Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the

No.	Recommended Security Measures[12]	Responsibility	AWS Considerations
			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.
	G1.2 Prepare a report	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 and monitoring visit, https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/. AWS has implemented a formal, documented incident response policy and program developed in alignment with ISO 27001 standards. For more information, please refer to the Incident Response section on the AWS: Overview of Security Processes whitepaper.
	G.1.3 Notification	Customer	Customers retain control and are responsible for their data, security controls and procedures. 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.
H. DEVELOPMENT ENVIRONMENTS Related to the definition of the development environment of data systems.			
H.1 Security of Development Environments	H.1.1 Implement a security development policy		AWS customers are responsible for implementing security development policies to satisfy organization-defined security requirements. And Customers retain control and are responsible for their data, security controls and procedures, including whether their content is masked, anonymized or encrypted. 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/.

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, among others, 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 https://aws.amazon.com/compliance and https://aws.amazon.com/security. Also, customers can review our Argentina Data Privacy website available at https://aws.amazon.com/compliance/argentina-data-privacy/.

Document Revisions

Date	Description
May 2018	First publication.
September 2020	Second publication.