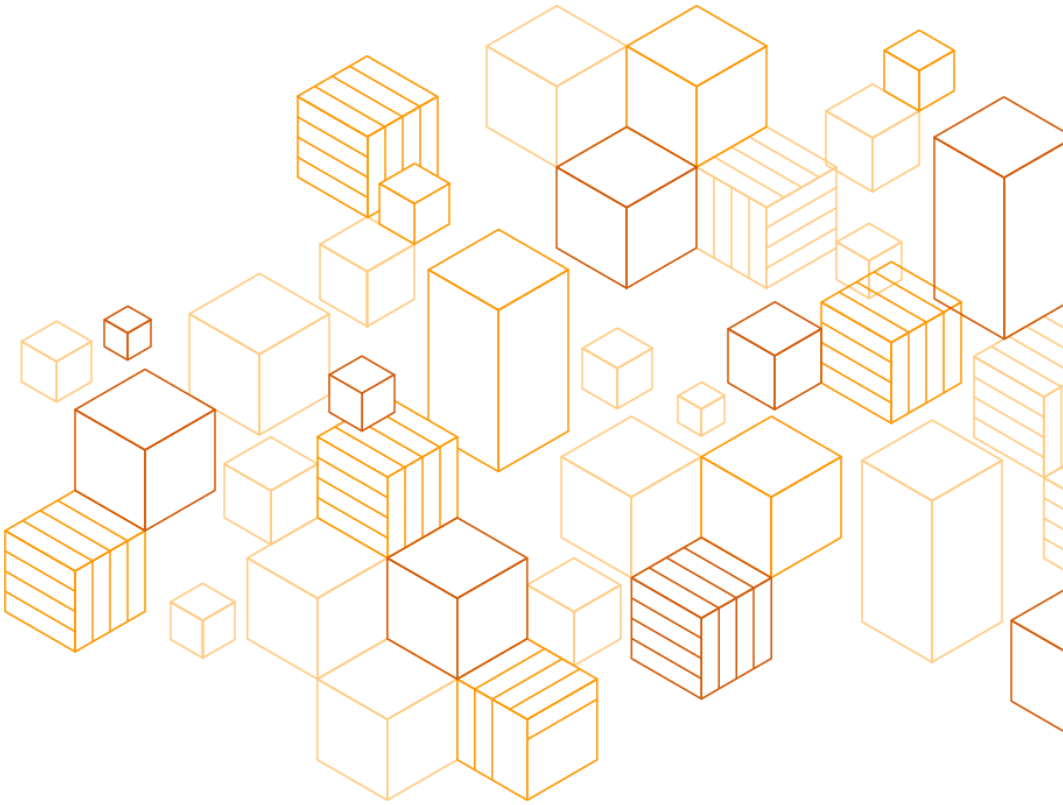
Navigating Indonesia Government Regulation No. 71 Considerations on AWS

Compliance Guide

Published May 17, 2021



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this Guide

AWS customers in Indonesia can now, without regulatory uncertainty, fully adopt the benefits of the AWS Cloud. This positive and highly anticipated clarification is a result of Government Regulation 71 Concerning the Operation of Electronic System and Transaction (GR 71), which amends the existing Government Regulation 82 of 2012 Concerning Electronic System and Transaction Operation (GR 82). GR 71 is effective as of 10 October 2019.

This paper discusses how customers can leverage AWS services and capabilities for their electronic systems and to safeguard customer content in the context of GR 71.

Overview

This paper provides information to assist customers in Indonesia who want to use AWS to run workloads and store or process customer content in the context of Indonesia's Government Regulation No. 71 of 2019 Concerning the Operation of Electronic System and Transaction ("**GR 71**"). Effective as of 10 October 2019, GR 71 revokes and replaces the Government Regulation 82 of 2012 Concerning Electronic System and Transaction Operation ("**GR 82**") and any conflicting implementing regulations of GR 82.

AWS customers in Indonesia can now, without regulatory uncertainty, fully adopt the benefits of the AWS cloud - one of the most flexible, reliable, and secure cloud computing environments available today. This positive and highly anticipated clarification is a result of GR 71. Most significantly, GR 71 clarifies that Electronic System Operators ("**ESO**") in Indonesia can transfer or store data offshore as further discussed in this paper. ESOs are any entities in Indonesia that manage or operate an electronic system, and can be either "private scope" or "public scope."

"Public Scope" ESOs include State Administrative Agencies i.e. legislative, executive, and judicial institutions at the central and regional level and other institutions that are formed by the provisions of legislation and any institution appointed by an Agency. Public Scope ESOs can store or process their data offshore, including by using an AWS Region outside Indonesia, during the two-year transition period starting from 10 October 2019. After October 2021, Public Scope ESOs will need approval from the Minister of Communications and Information Technology (KOMINFO) to store or process their data offshore.

"Private Scope" is defined generally and covers all businesses in Indonesia other than those that are a "State Administrative Agency." Private Scope ESOs can store or process all types of data outside Indonesia, including by using an AWS Region outside Indonesia.

This paper 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 AWS services and securing content stored on AWS in the context of GR 71

Scope

While GR 71 applies to both public scope and private scope ESOs, and AWS can help these ESOs meet their responsibilities and requirements in the Cloud, this paper focuses on typical questions asked by Public Scope ESOs when they are considering the implications of GR 71 on their use of AWS services. There will also be other relevant legal and policy considerations for each customer to address.

This paper is provided solely for informational purposes. It is not legal advice, and should not be relied on as legal advice. As each customer's requirements will differ, AWS strongly encourages its customers to obtain appropriate advice on their implementation of GR 71 requirements, and on applicable laws and other relevant requirements.

When we refer to *content* in this paper, we mean software (including virtual machine images), data, text, audio, video, images, and other content that a customer, or any end user, stores or processes using AWS services. For example, a customer's content includes objects that the customer stores using Amazon Simple Storage Service, 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 accounts, such as a customer's names, phone numbers, email addresses, and billing information—we refer to this as *account information* and it is governed by the AWS Privacy Policy. Our business changes constantly, and our Privacy Notice may also change. You should check our website frequently to see recent changes.

Overview of AWS services

AWS is the world’s most comprehensive and broadly adopted cloud platform, offering over 200 fully-featured services from data centres strategically located around the globe. Millions of customers - including the fastest-growing start-ups, largest enterprises, and leading government agencies - are using AWS to lower costs, become more agile, improve security, and innovate faster.

AWS has significantly more services, and more features within those services, than any other cloud provider–from infrastructure technologies like compute, storage, and databases–to emerging technologies such as machine learning and artificial intelligence, data lakes and analytics, and Internet of Things (IoT). This makes it faster, easier, and more cost effective to move your existing applications to the cloud and build nearly anything you can imagine.

AWS has the most extensive global cloud infrastructure. No other cloud provider offers as many Regions with multiple Availability Zones (AZs) connected by low latency, high throughput, and highly redundant networking. At the time of this paper's publishing, AWS has 77 AZs within 24 geographic regions around the world, and has announced plans for 18 more AZs and 6 more AWS Regions in Australia, India, Indonesia, Japan, Spain, and Switzerland. The AWS Region/AZ model has been recognized by Gartner as the recommended approach for running enterprise applications that require high availability. Gartner Research positions AWS in the Leaders quadrant of the new 2020 Magic Quadrant for Cloud Infrastructure & Platform Services (CIPS). CIPS, in the context of this Magic Quadrant, are defined as "standardised, highly automated offerings, in which infrastructure resources (e.g., compute, networking and storage) are complemented by integrated platform services." For additional information, visit https://pages.awscloud.com/GLOBAL-multi-DL-gartner-mq-cips-2020-learn.html.

Customer Content: Considerations relevant to privacy and data protection

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 how do I comply with these?

These considerations are not new and are not cloud-specific. They are relevant to internally hosted and operated systems as well as traditional third party hosted services. Each may involve storage of content on third party equipment or on third party premises, with that content managed, accessed, or used by third party personnel. When

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

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

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

AWS shared responsibility approach to managing cloud security

Is customer content secure?

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have distinct responsibilities in the operation and management of security. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for enabling and configuring AWS services for use and as necessary to meet compliance requirements. For example, when using infrastructure compute services such as Amazon Elastic Compute Cloud (EC2), the customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS-provided security group firewall and other security-related features. The customer will generally connect to the AWS environment through services acquired from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore part of the customer's area of

responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. Figure 1 shows the respective roles of the customer and AWS for infrastructure services in the shared responsibility model.

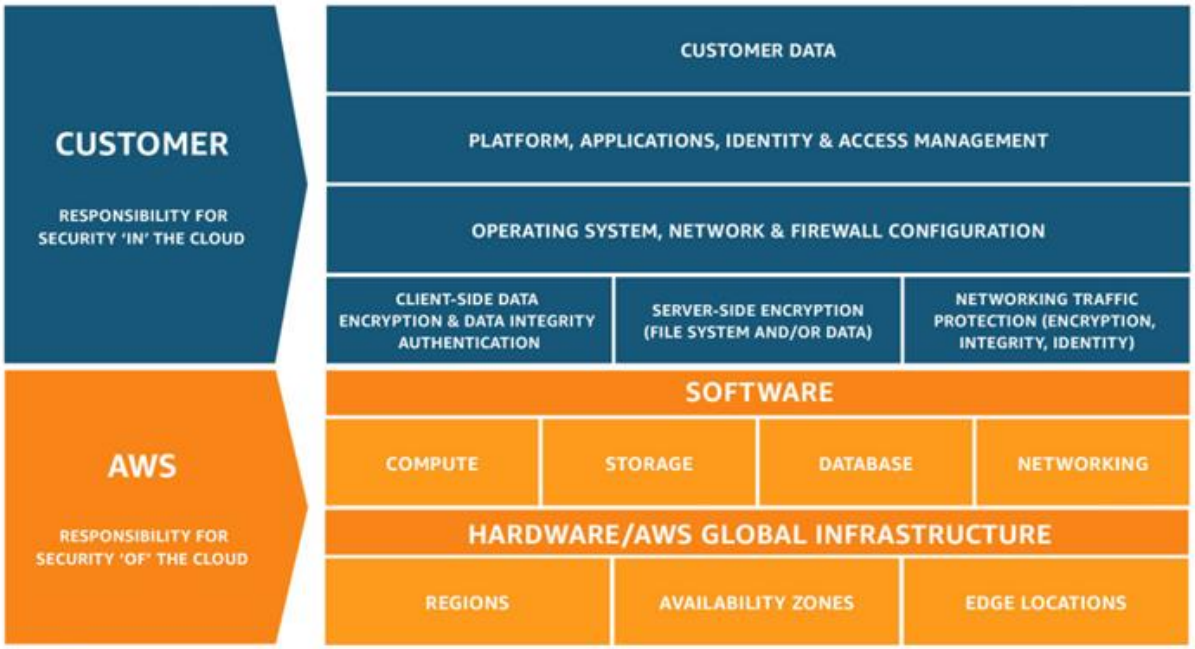


Figure 1: Shared responsibility model

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

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:

- Security measures that the cloud service provider (AWS) implements and operates – “security of the cloud”
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – “security in the cloud”

While AWS manages security ***of*** the cloud, security ***in*** the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, applications, systems, and networks – no differently than they would for applications in an on-site data centre.

Understanding security *OF* the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available, designed to provide optimum availability while providing complete customer segregation. It provides extremely scalable, highly reliable services that enable customers to deploy applications and content quickly and securely, at massive global scale.

Prior to choosing a location for our data centres, AWS performs initial environmental and geographic assessments. Data centre locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity.

Each AWS data centre is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur. Controls implemented to address environmental risks can include but are not limited to the following:

- AWS data centres are equipped with sensors and shutoff-valves to detect the presence of water. Mechanisms are in place to remove water in order to prevent any additional water damage.
- Automatic fire detection and suppression equipment to reduce risk and notify AWS Security Operations Centre, and emergency responders in the event of a fire. The fire detection system utilises smoke detection sensors in all data centre environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.
- Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centres are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilises free cooling as primary source of cooling when and where it is available based on local environmental conditions.
- AZs are physically separated within a metropolitan region and are in different flood plains. Each AZ is designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of a failure.

- The AWS data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. Power to AWS data centres is provided through local power provider(s). In the event of disruption, Uninterruptible Power Supply units provide back-up power or critical and essential loads in the facility and generators are used to provide back-up power for the entire facility.

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

We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorised access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System & Organization Control (SOC) 1, 2 and SOC 3 reports, ISO 27001, 27017, 27018 and 9001 certifications and PCI DSS Attestation of Compliance. Our ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls. AWS compliance certifications and reports can be requested at https://aws.amazon.com/compliance/contact. More information on AWS compliance certifications, reports, and alignment with best practices and standards can be found at AWS's compliance site.

Understanding security *IN* the cloud

Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to store or process using AWS services, only the customer can determine what level of security is appropriate for the content they store and process using AWS. Customers also have complete control over which services they use and whom they empower to access their content and services, including using Identity and Access Management (IAM) tools to apply the appropriate permissions.

Customers control how they configure their environments and secure their content, including using encryption tools to conform to best practices like encryption end to end, and key management system. AWS offers a range of options to simplify encryption and key management. AWS does not change customer configuration settings, as they are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures will be implemented in the cloud, in accordance with each customer's business needs. For example, if a robust degree of high availability architecture is required to protect customer content, the customer may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to customer content is required, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.

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

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

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

AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service

and AWS CloudTrail. To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and execute security assessments of their organisation's use of AWS services, AWS publishes a number of whitepapers relating to security, governance, risk, and compliance; and a number of checklists and best practices. Customers are also free to design and execute security assessments according to their own preferences, and can conduct vulnerability scans of their cloud infrastructure as long as those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy.

AWS Regions: Where is content stored?

AWS data centres are built in clusters in various global regions. We refer to each of our data centre clusters in a given country as an AWS Region. Each AWS Region consists of multiple, isolated, and physically separated Availability Zones (AZ) within a geographic area. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. Customers focused on high availability can design their applications to run in multiple AZs to achieve greater fault-tolerance.

Customers have access to a number of AWS Regions around the world, including Asia Pacific (Singapore) and a future region announced for Indonesia. Customers can choose to use one Region, all Regions, or any combination of AWS Regions. Customers can also centrally restrict use to only specifically designated Regions. For a map of AWS Regions, see https://aws.amazon.com/about-aws/global-infrastructure/.

AWS customers choose the AWS Region or Regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in Indonesia can choose to deploy their AWS services exclusively in one AWS Region, such as the Asia Pacific (Singapore) Region, if this is their preferred location. If the customer makes this choice, AWS will not move their content from Singapore without the customer's consent, except as legally required.

How can customers select their Region(s)?

Customers can select their regions through the management console, or programmatically, through API call.

Figure 2 provides an example of the AWS Region selection menu presented to customers when uploading content to an AWS storage service or provisioning compute resources using the AWS Management Console.

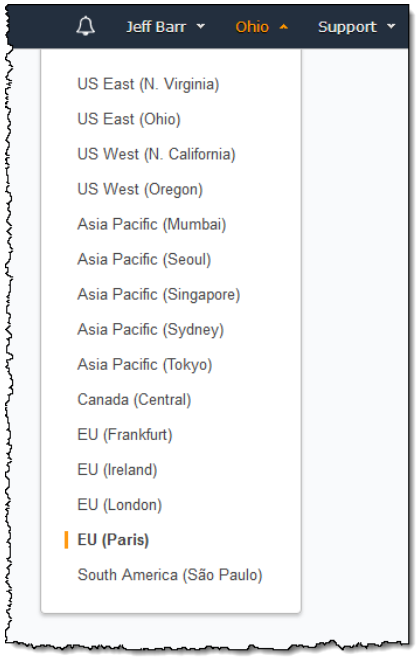


Figure 2 – Selecting AWS Global Regions in the AWS Management Console

Customers can also prescribe an AWS Region 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.

Compute and other resources launched by the customer into the VPC will be located in the AWS Region designated by the customer. For example, by creating a VPC in the Asia Pacific (Singapore) Region and providing a link (either a VPN or Direct Connect) back to the customer's data centre, all compute resources launched into that VPC would only reside in the Asia Pacific (Singapore) Region. This option can also be leveraged for other AWS Regions.

AWS has announced that it is working on the new AWS **Asia Pacific** (**Jakarta**) Region in Indonesia, based in **Greater Jakarta**, which is expected to arrive by the end of 2021 / early 2022. This Region comprises three AZs, which will give AWS customers broader

options for managing their data both onshore in Indonesia and offshore, and serve millions of end-users across Asia Pacific with even lower latency.

Transfer of Personal Data Cross Border

In 2016, the European Commission approved and adopted the new General Data Protection Regulation (GDPR). The GDPR replaced the EU Data Protection Directive, as well as all local laws relating to it. All AWS services comply with the GDPR. AWS provides customers with services and resources to help them comply with GDPR requirements that may apply to their operations. These include AWS's adherence to the CISPE code of conduct, granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards, and AWS's C5 attestations. For additional information, please visit the AWS General Data Protection Regulation (GDPR) Center and see our Navigating GDPR Compliance on AWS Whitepaper.

When using AWS services, customers may choose to transfer content containing personal data cross border, and they will need to consider the legal requirements that apply to such transfers. AWS provides a Data Processing Addendum that includes the Standard Contractual Clauses 2010/87/EU (often referred to as "Model Clauses") to AWS customers transferring content containing personal data (as defined in the GDPR) from the EU to a country outside of the European Economic Area (EAA), such as Indonesia. With our EU Data Processing Addendum and Model Clauses, AWS customers can transfer personal data with the knowledge that it will be given the same high level of protection it received in the EAA. The AWS Data Processing Addendum is incorporated in the AWS Service Terms and applies automatically to the extent the GDPR applies to the customer's processing of personal data on AWS.

Who Can Access Customer Content?

Customer Control Over Content

Customers using AWS maintain and do not release effective ownership or 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 AWS 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 and at rest; and also provides customers with the option to manage their own encryption keys or use third party encryption mechanisms of their choice
- Manage other access controls, such as identity, access management, permissions and security credentials

This allows AWS customers to control the entire life-cycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention, and disposal.

AWS access to customer content

AWS makes available to each customer the compute, storage, database, networking or other services, as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features (such as AWS Key Management Service), managing their own encryption keys, or using a third-party encryption mechanism of their choice. AWS does not access or use customer content without the customer's consent, except in the performance of our contractual obligations to customers or as legally required. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

Government rights of access

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

On March 23, 2018, United States Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), updating the legal framework for United States law enforcement requests for data stored on the servers of communication and cloud service providers. The CLOUD Act recognizes the right of cloud providers to challenge requests that conflict with another country's laws or national interests and requires that

governments respect local rules of law. Additionally, foreign governments concerned about the risk of government data disclosure may be entitled to sovereign immunity. The United States recognizes that under the principle of sovereign immunity foreign governments have effective legal means under U.S. law to prevent disclosure of their data. For additional information, see https://aws.amazon.com/compliance/cloud-act/.

AWS policy on granting government access

AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies typically must use recognised international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the Amazon Information Requests Portal online.

GR 71 Mapping

This part of the paper focuses on key aspects of GR 71 applicable to Public Scope ESOs when using AWS services. We also discuss aspects of the AWS Services which can help public sector customers navigate GR 71 compliance. Some of the considerations set out here may also be applicable to Private Scope ESOs.

Article	Summary of GR 71 requirements	Considerations
1 and 2	These 2 Articles contain the definitions for interpretation of GR 71. Public Scope ESO means the operation of Electronic System by State Administrative Agency or other agency appointed by the State Administrative Agency. State Administrative Agency is a legislative, executive, and judicial institution at the central and regional level and other institution that is formed by provisions of legislation.	**Customer:** Public sector customers which are a legislative, executive, and judicial institution at the central and regional level, or entities which are formed by provisions of legislation are considered Public Scope ESO. State owned enterprises are considered Private Scope ESO, unless otherwise appointed by a State Administrative Agency.

3 and 4	Every ESO should operate Electronic System reliably and safely and be responsible for its Electronic System's operation. Every ESO should operate an Electronic System that meets the minimum requirements to (a) re-display the Electronic Information and/or Electronic Document during the retention period; (b) protect the availability, integrity, authenticity, confidentiality, and accessibility of the Electronic Information; (c) operate in accordance with its procedures or instructions; …	**Customer:** Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have the complete freedom and control to design and build their security architecture to meet GR 71 requirements and other compliance needs. **AWS:** AWS is frequently used to meet one or more of over 90 national and international standards such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Special Publication 800-53 security controls, the International Standards Organization (ISO) 27001/27017/27018, Service Organization Controls (SOC), Payment Card Industry Data Security Standard (PCI DSS), and many more. AWS has developed two frameworks to help customers translate their business, security, and compliance requirements to the Cloud, and architect to take advantage of unique cloud opportunities. The first framework is the AWS Cloud Adoption Framework (CAF), which helps organizations plan for a successful cloud migration, and not just the technical aspects for a single application lift-and-shift, but with the intent to establish an organizational foundation to facilitate deploying, operating, and securing workloads at scale. This may include establishing a DevSecOps culture and processes, training staff and incorporating new paradigms into assignments and work, building shared cloud infrastructure and management service environments, implementing central governance and logging, and other aspects that will integrate with individual applications and use cases. The second framework is the AWS Well-Architected Framework, which helps you understand considerations and key decision points for building systems on AWS— it is a framework for guiding and evaluating your individual workload architectures. By using AWS Well-Architected, you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-

Article	Summary of GR 71 requirements	Considerations
		effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement. The AWS Well-Architected Framework started as a single whitepaper but has expanded to include domain-specific lenses, hands-on labs, and the AWS Well-Architected Tool. The AWS WA Tool, available at no cost in the AWS Management Console, provides a mechanism for regularly evaluating your workloads, identifying high risk issues, and recording your improvements. The user guides and admin guides for all AWS services can be found at http://aws.amazon.com/documentation (and any successor or related locations designated by AWS).
5	ESO should ensure its Electronic System does not contain any Electronic Information and/or Electronic Document that is prohibited in accordance with applicable legislation or facilitate the dissemination of the same.	**Customer:** Customers maintain full control of their content and responsibility for configuring access to AWS services and resources. Customers also remain responsible for complying with applicable compliance laws and regulations in relation to its content. **AWS:** In the context of customer content, AWS does not monitor or know what content is uploaded by the customer and does not control that content. We do not access, copy, move, or use your content for any purpose without your consent. AWS does offer tools to customers that can help identify when and where sensitive data is stored in AWS, such as Amazon Macie. This service uses machine learning and pattern matching to cost efficiently discover sensitive data at scale. Macie automatically detects a large and growing list of sensitive data types, including personal identifiable information (PII) such as names, addresses, and credit card numbers. The service also allows customers to define their own custom sensitive data types so they can discover and protect the sensitive data that may be unique to their business or use case.

Article	Summary of GR 71 requirements	Considerations
7	Hardware used by ESO should (a) meet the security, interconnectivity and compatibility aspects with the system used; (b) have technical, maintenance and/or aftersales support services from the provider; and (c) have guaranteed continuity of service. Compliance of the above should be carried through certification or other similar evidences.	**Customer:** Customer remains responsible for any hardware used to access and/or connect with AWS Cloud services. **AWS:** Under the shared responsibility model, AWS is responsible for protecting the physical 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. This shared model can help relieve the 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 AWS Cloud services operate. With the AWS Cloud, customers do not buy or lease hardware, but procure a service utility. Each AWS service is designed to meet specific service level agreement (SLA) objectives, such as Amazon S3 with a monthly availability commitment of at least 99.9%. AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for government and beyond. For more detailed information about the AWS certification programs, reports, and third-party attestations, visit the AWS Compliance Program webpage. You can also visit the AWS Services in Scope webpage for service-specific information.

Article	Summary of GR 71 requirements	Considerations
8	Software used by ESO should (a) be guaranteed of security and reliability as appropriate; and (b) ensure continuity of its services	**Customer:** Under the shared responsibility model for infrastructure compute services, the customer assumes responsibility and management of the guest operating system (including updates and security patches) and other third-party or custom-built application software, in addition to the configuration of the AWS-provided security group firewall. We recommend that customers carefully consider the AWS services and third-party software they choose to employ because their responsibilities vary depending on the AWS services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance their security and/or meet their more stringent compliance requirements by leveraging technology such as third-party host-based firewalls or host-based intrusion detection and prevention, and AWS encryption and key management. This shared responsibility model also extends to IT controls, namely the management, operation, and verification of IT controls. Customers can use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. Customers may refer to the AWS Well-Architected Framework to help build secure, high performing, resilient, and efficient infrastructure for their applications and workloads. **AWS:** AWS provides a wide range of information about its IT control environment to customers through technical papers, reports, certifications, and other third-party attestations. This documentation helps customers to understand the controls in place, relevant to the AWS services they use, and how those controls have been validated. This information also helps customers account for and validate that controls in their extended IT environment are operating effectively.

Article	Summary of GR 71 requirements	Considerations
11	ESO should guarantee: (a) availability of service level agreement (SLA); (b) availability of information security agreement on the Information Technology services used; … ESO should guarantee that each component and integration of all Electronic System are operating as appropriate.	**Customer:** Customers may refer to the AWS Cloud Adoption Framework and Well-Architected Framework to help build secure, high performing, resilient, and efficient infrastructure for their applications and workloads to meet their availability requirements. Customers can also leverage AWS services such as Amazon CloudTrail and CloudWatch to collect activity logs and generate events/alerts to ensure that all ESO components are working as designed. **AWS:** AWS provides SLAs for certain services. Each service has its own SLA calculation as detailed in the AWS SLAs page at https://aws.amazon.com/legal/service-level-agreements/. AWS contractually commits to implement reasonable and appropriate measures designed to help customers secure their content against accidental or unlawful loss, access, or disclosure.

13	ESO should have governance policy, operating work procedure and audit mechanism that are carried out periodically on an Electronic System.	**Customer:** This is a customer consideration. Customers may use the following AWS services to enable its governance of the Electronic System: • AWS Organizations to programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts. • AWS Config to immediately discover all of your AWS resources and view the configuration of each. You can receive notifications each time a configuration changes and dig into the configuration history to perform incident analysis. Customers may use the following AWS services to self-audit their Electronic System: • AWS Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the “all hands on deck” manual effort that often happens for audits and enable you to scale your audit capability in the cloud as your business grows. With Audit Manager, it is easy to assess if your policies, procedures, and activities – also known as controls – are operating effectively. • Amazon CloudWatch, a monitoring service for AWS cloud resources and the applications customers run on AWS and on-premises. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in AWS resources. Customers can also monitor custom metrics generated by customer own applications and services. • AWS CloudTrail to provide logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS Cloud service.

Article	Summary of GR 71 requirements	Considerations
		The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing. • AWS Personal Health Dashboard provides a personalized view into the performance and availability of the AWS Cloud services you are using and alerts that are automatically triggered by changes in the health of those services. AWS Trusted Advisor is a convenient way for you to see where you could use a little more security. It monitors AWS resources and alerts you to security configuration gaps such as overly permissive access to certain Amazon Elastic Compute Cloud (Amazon EC2) instance ports and Amazon S3 storage buckets, minimal use of role segregation using IAM, and weak password policies. This service is provided automatically when you sign up for the Business support plan from AWS Support. **AWS:** The AWS Compliance Program helps customers and governments understand the robust governance, risk management, and controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to get established and start to operate in an AWS security control environment.

14(1)	ESO should implement Personal Data protection principle in processing Personal Data, including: Collection is carried out in limited and specific manner, legally valid, fair and with the knowledge and consent of the Personal Data owner; Processing is carried out in accordance with intended use; Processing is carried out by guaranteeing the Personal Data owner's right; Processing is carried out with accuracy, completeness, not misleading, up to date, can be accounted for, and with due regard to the purpose of processing; Processing is carried out with protecting the security of Personal Data from loss, misuse, unauthorized access and disclosure, and alteration or destruction; Processing is carried out by informing the purpose of collecting, processing activity, and the failure in protection; Personal Data is destroyed and/or deleted unless still in a retention period in accordance with applicable legislation	**Customer:** Customers are responsible for security in the cloud, including security of their content (and personal data included in their content). The customer determines what, if any, personal data they store and process in AWS, and retains full ownership and control of that data to implement required data protections, monitor for unauthorized access and abuse, and to respond to suspicious events. The customer determines how and what personal data will be collected, ensuring it is limited and specific to their use case, that its collection is legal and fair, that it is retained only for the period required, that it is destroyed when required, and that the corresponding individuals are aware and consent to their personal data being collected and used in such a way as to protect their rights in accordance with GR 71 and other applicable laws, regulations, and policies. The customer controls the format and structure of its content, and how it maintains the confidentiality, integrity, and availability of that content. The customer can implement data protection through encryption in transit and at rest. AWS encryption modules are US Federal Information Processing Standard (FIPS) 140-2 compliant, with key management provided by AWS CloudHSM (FIPS 140 Level 3 validated) or AWS Key Management Service (FIPS 140 Level 2 validated). Encryption in transit can be facilitated by AWS Certificate Manager. There are also other AWS services, such as AWS Config, that can enforce encryption to prevent human error. And the customer chooses who, when, and how personal data will be shared and disclosed with other entities, and in accordance with all applicable laws, regulations, and policies. In addition to data protection capabilities provided by AWS, the customer has access to AWS and third-party tools that provide the visibility and detection capabilities for the customer to detect and respond to suspicious activity. The customer owns the relationship with the private entities whose personal data they collect, store, and process in AWS. This

Article	Summary of GR 71 requirements	Considerations
		relationship includes the responsibility to inform private entities of the intent and reason to collect personal data, describe the scope for its use, respond to inquiries about the collection and protection of the personal data, and any notifications due to a lapse in data protection. **AWS:** AWS does not collect personal data, directly, or indirectly through content a customer stores or processes in AWS. AWS does not have a direct relationship with the individuals whose personal data is stored or processed by a customer using AWS, and is not aware of the scope or use of that data. AWS does not access or use customer content, which may include personal data, for anything other than providing the AWS services the customer employed. Therefore, AWS is not required and is unable to communicate with the relevant individuals about their personal data stored or processed in AWS. AWS is responsible for managing the security of the underlying cloud environment. For a complete list of all the security measures built into the core AWS cloud infrastructure, and services, see Best Practices for Security, Identity & Compliance on AWS Architecture Center. 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 Attestation of Compliance.
14(3) and (4)	Personal Data Processing should meet the requirement of legal consent from Personal Data owner for one or several specific purposes that have been informed to the Personal Data Owner. In addition, Personal Data processing should meet the conditions required in Article 14(4).	Please refer to input for Article 14(1) above.

Article	Summary of GR 71 requirements	Considerations
14(5)	In the event of failure in the Personal Data protection it manages, ESO should notify in writing the Personal Data owner.	**Customer:** 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. Customers control credentials, and determine who is authorized to access their AWS account. AWS does not have visibility into customer credentials, or who is and who is not authorized to log into an account. Therefore, the customer is responsible for monitoring use, misuse, distribution, or loss of their credentials. In some jurisdictions it is mandatory to notify individuals or a regulator of unauthorized access to or disclosure of personal data, and there are circumstances in which notifying individuals will be the best approach in order to mitigate risk, even though it may not be mandatory under the applicable law. It is for the customer to determine when it is appropriate or necessary to notify individuals and which notification process they will follow. Customers can leverage AWS services such as AWS CloudTrail, AWS Virtual Private Cloud (VPC FlowLogs, Amazon CloudWatch, Amazon EventBridge, Amazon GuardDuty, and AWS Security Hub to log user activities and network traffic, detect anomalies and suspicious activity, and correlate events to identify the possibility of data compromise.

Article	Summary of GR 71 requirements	Considerations
15	Every ESO obliged to erase irrelevant Electronic Information and/or Electronic Document which under its control by the request of the relevant person. The obligation to erase irrelevant Electronic Information and/or Electronic Document consists of: (a) right to erasure; … ESO who obliged to erase Electronic Information and/or Electronic Document is the ESO that obtains and/or processes the Personal Data under its control.	**Customer:** The customer retains ownership and control of their content stored or processed in AWS, including control over how that content is secured and who can access and amend or delete that content. In addition, as between the customer and AWS, the customer has a relationship with the individuals whose personal data is included in customer content stored or processed in AWS services. The customer rather than AWS is therefore able to receive requests by relevant individuals to erase personal data included in customer content. Customers can leverage AWS service features such as Amazon S3 storage lifecycle management to assign the stages of their data storage that automatically moves data from active use in Amazon S3, to archival in Amazon S3 Glacier, and then deletes the data based on last-activity and timeline thresholds determined by the customer. **AWS:** AWS only uses customer content to provide the AWS services selected by each customer to that customer, and AWS has no contact with the individuals whose personal data is included in content a customer stores or processes using the AWS services. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to provide such individuals with access to, or the ability to erase, their personal data.
16	Definition of irrelevant Electronic Information and/or Electronic Document	Please refer to input for Article 15 above.
18	Every ESO is obliged to provide erasure mechanism of irrelevant Electronic Information and/or Electronic Document in accordance with applicable legislation.	Please refer to input for Article 15 above.

Article	Summary of GR 71 requirements	Considerations
19	ESO should implement a good and accountable Electronic System's governance which at least meet the following requirements: a) The availability of procedure or instruction in Electronic System Operation that is documented and/or announced in understandable language, information or symbol by the parties related to the Electronic System Operation; b) The availability of a sustainable mechanism in maintaining the novelty and clarity of the implementing guideline's procedure; c) The availability of institution and complete supporting personnel for the operation of Electronic System as appropriate; d) The performance management should be implemented in the Electronic System to ensure that the Electronic System is operating as appropriate; and e) The availability of a plan on ensuring the continuity of the Electronic System Operation it manages.	**Customer:** This is the customer's responsibility as set out in the shared responsibility model. Customers may refer to the AWS Cloud Adoption Framework and AWS Well-Architected Framework to help build secure, high performing, resilient and efficient infrastructure for their applications and workloads. Customers can leverage AWS services and features, such as: • AWS management and governance services, so that the customer does not have to choose between innovation and control—you can have both. Customers choose AWS to help manage and govern their AWS and non-AWS resources. With AWS, customers can enable, provision, and operate their environment for both business agility and governance control. • Documentation for all AWS services. Four kinds of management tools (provisioning, operations management, monitoring and logging, and managed services for configuration management) that work together and are integrated with every part of the AWS Cloud from Amazon EC2 to DynamoDB, in order to allow customers to control all parts of their cloud infrastructure. **AWS:** AWS manages a governance and risk management program which is built to manage highly dynamic cloud resources at massive scale. We leverage automation to the greatest extent possible to ensure consistent and reliable outcomes that are realized faster than what people can perform. AWS governance program and tasks are frequently audited by third-parties and included in our attestations found in AWS Artifact.

Article	Summary of GR 71 requirements	Considerations
20(1)	Public Scope ESO should have an activity's continuity plan to deal with disturbance or disaster in accordance with the risk of the impact caused.	**Customer:** AWS offers a unique opportunity for customers to overcome traditional challenges with BCM where the physical facilities are limited or the complexity and costs of architecting for high availability and disaster recovery are too high. Customers can architect and build highly resilient applications on AWS with automatic failover and load balancing, encrypted backups in alternate regions or data centres, and the ability to rapidly redeploy AWS architectures and resources through the use of infrastructure as code templates. With AWS, customers can transform the historical concept of business continuity and disaster recovery to a level not before imagined in a traditional data centre or co-location service providers. Customers can reference the Reliability Pillar in the AWS Well-Architected Framework to help them design and implement a resilient architecture, leveraging AWS infrastructure and services such as AWS Regions and Availability Zones, AWS Elastic Load Balancing, Amazon EC2 Auto-Scaling Groups, AWS Backup, and AWS CloudEndure. **AWS:** AWS performs BCM to ensure people and process continuity across the globe, which is validated via the SOC attestation and ISO 27001 certification schemes.

20(2)	Public Scope ESO is obliged to perform the managing, processing, and/or storing of Electronic System, and Electronic Data in the territory of Indonesia	**Customer:** The customer can choose the AWS Region or Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single Region if preferred. AWS services are structured so that a customer maintains effective ownership and control of customer content regardless of what Region they use for their content. Pursuant to Article 102(2), Public Scope ESO must ensure all Electronic System and Electronic Data reside in the territory of Indonesia by the end of the transition period in October 2021. AWS has announced that it is working on the AWS Asia Pacific (Jakarta) Region in Indonesia, based in Greater Jakarta and comprises three AZs, which will give AWS customers broader options for managing their data both onshore in Indonesia and offshore by end of 2021 / early 2022. For customers who prefer to run their workloads and applications locally even during the transition period, AWS offers hybrid services such as AWS Outposts, which is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any data centre, co-location space, or on-premises facility for a truly consistent hybrid experience. Customers can then use the AWS Cloud, where appropriate, as an extension of its own data centre. To further secure the network connectivity to AWS, a physical and private connection to AWS is highly recommended. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations, allowing on-premises data to be accessed securely from the AWS Cloud. **AWS:** AWS only stores and processes customers' content in the AWS Region(s), and using the services chosen by, the customer, and otherwise will not move customer content without the customer's consent, except as legally required. If a customer chooses to store content in more than one Region, or copy or move content between Regions, that is solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed.

Article	Summary of GR 71 requirements	Considerations
22	ESO is obliged to provide audit track record of the whole Electronic System Operation activities	Please see input to Article 13 above.

23, 24(1), (2)	ESO is obliged to perform security on Electronic System components. ESO is obliged to implement procedures and facilities on the security of Electronic System to avoid disruption, failure and loss; and provide a security system that includes procedure, preventive system, and countermeasure of threats and attacks that leads to disruption, failure and loss.	**Customers:** Please refer to the shared responsibility model discussed above and input for Articles 3, 4, 7, 8, 11, 13 and 19. AWS offers security and management services that can be employed, along with a wide selection of partner security offerings, for customers to protect, detect, and respond to security events. **AWS:** In relation to security OF the cloud: **Data Centre Access Monitoring:** We monitor our data centres using our global Security Operations Centres, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data centre access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses. **AWS Security Operations Centres Monitor Global Security:** AWS Security Operations Centres are located around the world and are responsible for monitoring, triaging, and executing security programs for our data centres. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data centre security teams. In short, they support our security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyse a potential security incident. **AWS Incident Response Policy:** AWS has implemented a formal and documented incident response policy and program which addresses purpose, scope, roles, responsibilities, and management commitment. AWS uses a three-phased approach to manage incidents: **Activation and Notification Phase:** Incidents for AWS begin with detection of an event. This can come from several sources including: (i) 24x7x365 monitoring and alarming of real time metrics and service dashboards (for majority of incidents); (ii) trouble tickets entered by an AWS employee; and (iii) calls to the 24x7x365 technical support hotline. **Recovery Phase:** The relevant resolvers will perform break fixes to address the incident. Once troubleshooting, break fixes, and

Article	Summary of GR 71 requirements	Considerations
		affected components are addressed, the call leader will assign next steps for follow-up documentation and actions and end the call engagement. **Reconstitution Phase:** Upon relevant fix activity completion, the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. Senior management will review results of the post mortem analysis, and relevant actions such as design changes, etc, will be captured in a Correction of Errors (COE) document and tracked to completion. In addition to internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. We maintain a Service Health Dashboard to alert customers to any issues that may be of broad impact. The AWS incident management program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001, and FedRAMP compliance.
24(3)	In the event of system failure or disruption that have serious impact caused by the action of other party to the Electronic System, the ESO is obliged to secure the Electronic Information and/or Electronic Document and report it at the first chance to the law enforcement and Ministry or Agency in concern.	Please refer to input for Articles 13, 14(5), 19, 23 and 24.
25, 26(1)	ESO is obliged to re-display Electronic Information and/or Electronic Document in their entirety in accordance with the stipulated format and retention period. ESO is obliged to protect the Electronic Information and/or Electronic Document in accordance with legislation.	Please refer to input for Articles 3, 4 and 5.
26(2)	The Electronic Information and/or Electronic Document should be unique and clarify its ownership	**Customer:** This is a customer responsibility. AWS customers retain ownership and control of their content.

Article	Summary of GR 71 requirements	Considerations
27	ESO should guarantee the functionality of Electronic System while taking into consideration the interoperability and compatibility with the previous Electronic System.	**Customer:** This is a customer responsibility. **AWS:** AWS offers the broadest set of global compute, storage, networking, database, analytics, application, deployment, management, and mobile services that help organizations move faster, lower IT costs, and scale applications. AWS has been continually expanding its services to support virtually any cloud workload, and we now have more than 175 services that serve millions of active customers every month through our 24 Regions, 77 AZs, 2 Local Zones, and 216 Points of Presence (205 Edge Locations and 11 Regional Edge Caches). AWS has also announced plans for three more AWS Regions in Indonesia, Japan, and Spain. AWS provides a suite of application integration services that enable communication between decoupled components within microservices, distributed systems, and serverless applications. You don't need to refactor your entire architecture to benefit - decoupling applications at any scale can reduce the impact of changes, making it easier to update and faster to release new features. You can use CloudHSM with Amazon Redshift, Amazon RDS for Oracle, or third-party applications (such as SafeNet Virtual KeySecure) as your Root of Trust, Apache (SSL termination), or Microsoft SQL Server (Transparent Data Encryption). You can also use CloudHSM when you write your own applications and continue to use the standard cryptographic libraries, including PKCS#11, Java JCA/JCE, and Microsoft CAPI and CNG.

Article	Summary of GR 71 requirements	Considerations
32(1)	Every person who works in the Electronic System operation environment is obliged to secure and protect the facilities and infrastructures of Electronic System or the relayed information through an Electronic System.	**Customer:** This is the customer's responsibility for security IN the cloud. **AWS:** In relation to security OF the cloud, our people help make your data safer. Every AWS employee, whether they work at a data centre or not, is trained to think security first -- that is our culture. Protecting your data is as important to us as it is to you. AWS provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff. Learn more at https://aws.amazon.com/compliance/data-center/controls/.

Article	Summary of GR 71 requirements	Considerations
99(3)	Agencies or institutions that have strategic Electronic Data must prepare Electronic Documents and electronic backups and connect them to certain data centres for the purpose of data security.	**Customer:** This is a customer responsibility. **AWS:** AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS. Using industry-standard 802.1q Virtual Local Area Networks (VLANs), this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS Cloud.
102(2)	Public Scope Electronic System Providers in Electronic System operating prior to the promulgation must adjust accordingly to Article 20(2) within a period of 2 years.	Please see input above for Article 20(2).
All other Articles not mentioned above including Articles 6, 9, 10, 12, 17, 28-31, 33-98, 100, 101, 103, 104		**Customer:** It is customer's responsibility to consider the requirements of these Articles as appropriate when operating an Electronic System or implementing an Electronic Transaction.

Public Sector Case Studies

The following is a selection of the latest Asia public sector case studies:

Indonesia

- Aksi Cepat Tanggap (ACT)
- WWF Indonesia
- Halodoc
- Binus University
- Diskominfo West Java

Singapore

- Genome Institute of Singapore
- Doctor Anywhere Pte Ltd
- Singapore University of Social Sciences
- Singapore Polytechnic

Malaysia

- Asia Pacific University
- Asia Pacific Institute of Information Technology (APIIT)
- Smart Selangor Digital Unit (SSDU)
- Apigate

Philippines

- AMA Education System
- Chinese General Hospital (CGH)
- International Rice Research Institute

Thailand

- CAT Telecom
- King Mongkut's Institute of Technology Ladkrabang (KMITL)
- Digital Economy Promotion Agency (DEPA)
- Doctor Raksa

Cambodia

- People in Need
- Tepmachcha

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.

AWS Artifact

Customers can review and download reports and details about more than 2,500 security controls using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS's security and compliance documents, including the ANDB Addendum and certifications from accreditation bodies across geographies and compliance verticals.

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS cloud and gain proficiency with AWS services and solutions. We offer free instructional videos, 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 the 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, contact AWS at: https://aws.amazon.com/contact-us/ or contact your local AWS account representative.

Contributors

Contributors to this document include:

- Agustinus Tobing, Head of Security Assurance, Indonesia, Amazon Web Services
- Jonathan Hatae, Senior Corporate Counsel, Amazon Web Services
- Michael South, Security & Compliance Business Acceleration Team, Amazon Web Services
- Samantha Low, Corporate Counsel, Amazon Web Services
- Shiv Chandran, Senior Corporate Counsel, Amazon Web Services

Document Revisions

Date	Description
May 17, 2021	First publication