International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives

Satyanarayan Kanungo

Submitted: 06/02/2024 **Revised**: 11/03/2024 **Accepted**: 18/03/2024

Abstract: Cloud computing has revolutionized how organizations store, process and share data. However, the use of cloud services introduces complex data privacy and compliance challenges from legal and regulatory standpoints. This paper explores the key data protection laws and regulations impacting cloud computing, including the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and industry-specific requirements like the Payment Card Industry Data Security Standard (PCI DSS). It examines the shared responsibility model between cloud providers and customers, jurisdictional considerations, international data transfers, vendor management, incident response obligations, and auditing/monitoring of cloud environments. The paper also discusses evolving trends such as the increased focus on data localization laws and the growing adoption of secure enclaves and confidential computing. Finally, it provides recommendations for organizations to navigate this complex landscape through robust governance frameworks, risk assessments, contractual safeguards with cloud service providers, and transparency with end-users. Effectively addressing data privacy and compliance issues is essential for organizations to reap the benefits of cloud computing while protecting sensitive information and upholding their legal and ethical duties.

Keywords: *cloud computing; data privacy; GDPR; CCPA; HIPAA; shared responsibility; data localization; confidential computing*

1. Introduction

The rapid adoption of cloud computing has transformed the IT landscape, providing organizations with unprecedented flexibility, scalability and cost efficiency. Gartner predicts that worldwide end-user spending on public cloud services will reach nearly $600 billion in 2023, a 21.7% growth from 2022 [1]. However, the use of cloud services often involves the storage and processing of vast amounts of sensitive data outside an organization's direct control, introducing complex privacy and compliance challenges.

Data protection laws and industry-specific regulations impose stringent requirements on how personal data and other sensitive information must be collected, used, shared and secured. Non-compliance can result in substantial fines, reputational damage, business disruption and legal action. For example, the EU's General Data Protection Regulation (GDPR), which came into effect in May 2018, authorizes penalties of up to €20 million or 4% of a company's global annual turnover for non-compliance [2]. In the US, the California Consumer Privacy Act (CCPA) which went into effect in January 2020, provides for civil penalties of up to $7,500 per intentional violation and $2,500 per unintentional violation [3].

Cloud computing introduces unique considerations from a legal and regulatory compliance standpoint. Data may be stored and processed in multiple geographic locations, potentially subjecting it to various jurisdictional requirements. The shared responsibility model between cloud providers and customers can create ambiguity around roles and obligations. Sensitive data could be exposed to unauthorized access by third party vendors or foreign governments. Lack of visibility and control over the cloud infrastructure complicates monitoring and auditing.

This paper examines the key data privacy and compliance issues associated with cloud computing and provides an in-depth analysis from legal and regulatory perspectives. It is structured as follows: Section 2 provides an overview of major data protection laws and regulations impacting cloud services. Section 3 explores jurisdictional challenges and considerations around cross-border data transfers. Section 4 discusses the shared responsibility model and its implications for compliance. Section 5 delves into supply chain risk management and vendor due diligence. Section 6 examines incident response and breach notification obligations. Section 7 covers auditing and monitoring requirements and best practices. Section 8 analyzes the growing trends of data localization and confidential

Independent Researcher, Principal Data Engineer,USA.
Email id: satyanarayankanungo2@gmail.com
orchid Id 0009-0009-5367-2680
https://www.linkedin.com/in/kanungosatyanarayan in

computing. Finally, Section 9 provides recommendations for organizations to manage data privacy and compliance risks in cloud environments.

2.Regulatory Landscape

2.1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in the European Union (EU) on May 25, 2018. It impacts any organization that collects, processes or stores the personal data of EU residents, regardless of the organization's location. Under GDPR, personal data is broadly defined as "any information relating to an identified or identifiable natural person" [4]. This includes not only direct identifiers like names and government ID numbers, but also online identifiers such as IP addresses, cookies, and device IDs when they can be tied to a specific individual.

GDPR sets out seven key principles relating to processing of personal data [5]:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

It grants data subjects specific rights, including the right to be informed, right of access, right to rectification, right to erasure ("right to be forgotten"), right to restrict processing, right to data portability, right to object, and rights related to automated decision making and profiling [6].

GDPR requires organizations to have a valid legal basis for processing personal data, such as obtaining explicit consent, fulfilling a contract, complying with a legal obligation, protecting vital interests, performing a task in the public interest, or pursuing legitimate interests that are not overridden by individual rights [7]. When relying on consent, it must be freely given, specific, informed and unambiguous [8]. Special categories of personal data, such as health information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and data concerning a person's sex life or sexual orientation are subject to even stricter requirements [9].

From a cloud computing perspective, GDPR has significant implications:

- Both cloud providers and their customers can be considered data controllers and/or processors, triggering various obligations around data subject rights, data retention, data security, breach notification, etc. [10]
- The cloud customer, as the data controller, must ensure there is a lawful basis for sending personal data to the cloud and that the cloud provider will comply with GDPR's requirements. This necessitates robust vendor due diligence and contractual safeguards.
- Cross-border data transfer restrictions apply when personal data originating in the EU is transferred to countries that have not been deemed to provide an adequate level of data protection. Transfers may still occur using mechanisms like Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or derogations for specific situations [11].
- Cloud providers must notify customers of data breaches without undue delay, and breach notifications to supervisory authorities and data subjects are subject to strict timelines [12].
- The data controller must conduct Data Protection Impact Assessments (DPIAs) when processing operations are likely to result in a high risk to the rights and freedoms of data subjects, such as when moving sensitive data to the cloud [13].
- Data residency requirements may dictate that personal data must be stored and processed only in specific countries or regions.

2.2. California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, is considered one of the most comprehensive state privacy laws in the US. It applies to for-profit companies doing business in California that meet one of the following thresholds: (a) annual gross revenue above $25 million; (b) annually buys, receives, sells, or shares personal information of 50,000 or more California residents, households, or devices; or (c) derives 50% or more of annual revenue from selling California residents' personal information [14].

CCPA grants California residents rights similar to GDPR, including the right to know what personal information is collected, used, shared or sold, the right to request deletion of personal information, the right to opt-out of sale of personal information, and the right to non-discrimination for exercising these rights [15]. It defines personal information broadly as "information

that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" [16].

CCPA requires businesses to provide notice to consumers at or before data collection [17]. Consumers have the right to request that a business disclose what categories and specific pieces of personal information it has collected, the sources from which that information was collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information was shared [18]. Upon receiving a verifiable consumer request, businesses must promptly take steps to disclose and deliver, free of charge, the personal information required [19].

For cloud computing, key considerations under CCPA include:

- Identifying whether the business or its cloud provider is subject to CCPA based on the thresholds
- Determining what personal information is collected and stored in the cloud, and properly disclosing this in notices and privacy policies
- Putting processes in place to handle consumer access and deletion requests when data resides in the cloud
- Having contractual safeguards and due diligence to ensure cloud providers comply with CCPA obligations
- Understanding and complying with restrictions on the sale of personal information

Importantly, the definition of "sale" under CCPA is extremely broad. It includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration" [20]. This could potentially include transfers of personal data to cloud providers, necessitating careful analysis.

In November 2020, California voters approved Proposition 24, also known as the California Privacy Rights Act (CPRA). CPRA amends and expands CCPA, with most provisions going into effect on January 1, 2023 [21]. Notably, CPRA extends CCPA's requirements to a new category of "sensitive personal information," imposes additional contractual requirements for transfers of personal information to third parties, and establishes the California Privacy Protection Agency to implement and enforce the law [22].

2.3. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is the primary US law regulating the security and privacy of protected health information (PHI). PHI is defined as individually identifiable health information transmitted or maintained in any form or medium by a covered entity or its business associates [23]. Covered entities include health plans, healthcare providers, and healthcare clearinghouses. Business associates are persons or entities that perform certain functions or activities on behalf of, or provide certain services to, a covered entity involving the use or disclosure of PHI [24].

The HIPAA Privacy Rule sets national standards for the protection of PHI, including how it may be used and disclosed by covered entities. It generally prohibits the use or disclosure of PHI without the individual's authorization unless it is for treatment, payment, or healthcare operations, or falls under another exception [25]. The HIPAA Security Rule establishes safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic PHI (ePHI). This includes administrative, physical, and technical safeguards [26].

When a covered entity engages a cloud service provider (CSP) to create, receive, maintain or transmit ePHI on its behalf, the CSP is considered a business associate under HIPAA [27]. This triggers several obligations:

- The covered entity must enter into a business associate agreement (BAA) with the CSP, specifying each party's responsibilities and liabilities with respect to the ePHI [28].
- The CSP must comply with the applicable provisions of the HIPAA Security Rule, including implementing appropriate administrative, physical, and technical safeguards to protect the ePHI [29].
- The CSP must ensure that any subcontractors it engages to assist in its work for the covered entity agree to the same restrictions and conditions that apply to the CSP [30].
- The CSP must report any security incidents or breaches of unsecured PHI to the covered entity [31].
- The CSP must make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the CSP on behalf of, the covered entity available to the Secretary of Health and

Human Services for purposes of determining the covered entity's compliance with HIPAA [32].

Covered entities are ultimately responsible for ensuring their PHI is protected when using cloud services. They must exercise due diligence in selecting and monitoring CSPs, ensuring that robust BAAs are in place, and understanding the CSP's security controls and practices. Key considerations include data encryption, access controls, auditing and monitoring capabilities, backup and disaster recovery processes, and the geographic location of data storage and processing.

HIPAA violations can result in significant financial penalties. The four tiers of violations and their corresponding penalty amounts were strengthened in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act. As of 2021, penalties range from $127 per violation (with an annual maximum of $31,500) for tier 1 violations, to $59,522 per violation (with an annual maximum of $1,785,651) for tier 4 violations [33]. Certain violations may also carry criminal charges.

2.4. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. It was developed by the PCI Security Standards Council, an independent body created by the major payment card brands (Visa, MasterCard, American Express, Discover, and JCB) [34].

PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. The current version, PCI DSS 4.0, released in March 2022, consists of 12 core requirements and over 400 test procedures [35]:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Protect all systems against malware and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need to know
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

PCI DSS has evolved to address the growing use of cloud computing. The PCI Security Standards Council has published guidelines on cloud computing to help organizations understand their PCI DSS responsibilities when using cloud services [36]. Key considerations include:

- Scoping: Identifying which cloud computing components are in scope for PCI DSS, based on how the cloud service is used and how cardholder data is stored, processed, or transmitted.
- Responsibility: Determining the PCI DSS responsibilities of the cloud provider and the client. The exact allocation depends on the service model (IaaS, PaaS, SaaS) and the specific services used.
- Segmentation: Isolating the CDE (cardholder data environment) from other cloud components that do not store, process, or transmit cardholder data or provide security functions.
- Data protection: Ensuring that cardholder data is protected in accordance with PCI DSS requirements, including encryption, access controls, and data retention policies.
- Security controls: Verifying that the cloud provider has implemented and validated the necessary security controls, either directly or through the use of compliant third-party services.

Organizations that use cloud services must include the cloud provider in their PCI DSS assessment scope. They must understand which PCI DSS requirements the cloud provider fulfills and which requirements they are responsible for themselves. This allocation of responsibilities should be clearly defined in contracts and service level agreements (SLAs).

Compliance with PCI DSS is enforced through a combination of self-assessments and, for larger or more complex environments, external audits by Qualified Security Assessors (QSAs). Non-compliance can result in fines, increased transaction fees, and even termination of the ability to accept payment cards.

3.Jurisdictional Considerations and Cross-Border Data Transfers

3.1. Jurisdictional Challenges

Cloud computing inherently involves the storage and processing of data across multiple geographic locations, often crossing jurisdictional boundaries. This can create complex legal and regulatory challenges, as different countries and regions have their own data protection laws with varying requirements.

The primary jurisdictional considerations in cloud computing relate to:

- Applicable laws: Determining which country's or region's laws apply to the data, based on factors such as the location of the data subject, the location of the data controller or processor, and the location of the data storage and processing.
- Conflicts of law: Resolving situations where the laws of multiple jurisdictions apply and potentially conflict with each other.
- Enforcement: Ensuring compliance with applicable laws and dealing with enforcement actions by regulatory authorities in different jurisdictions.
- Data sovereignty: Addressing concerns about foreign governments accessing data stored in their jurisdiction, either through legal means such as subpoenas or court orders, or through covert intelligence gathering.

The CLOUD Act (Clarifying Lawful Overseas Use of Data Act), enacted in the United States in 2018, highlights some of these challenges. The CLOUD Act amends the Stored Communications Act (SCA) to allow US law enforcement to compel US-based technology companies, via warrant or subpoena, to provide data stored on servers regardless of whether the data is stored in the US or in foreign countries [37]. This has raised concerns about potential conflicts with foreign data protection laws, particularly the GDPR. The CLOUD Act does allow companies to challenge requests that would require them to violate the laws of a foreign government, but the process for resolving such conflicts is not yet clear [38].

3.2. Cross-Border Data Transfer Mechanisms

Given the global nature of cloud computing, it's crucial for organizations to understand and comply with cross-border data transfer restrictions. These restrictions are most prominent in the EU, where the GDPR sets strict conditions for transferring personal data outside the European Economic Area (EEA).

Under the GDPR, personal data can only be transferred to countries that the European Commission has determined to provide an adequate level of data protection. As of 2021, the Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection [39].

For transfers to other countries, organizations must use one of the following transfer mechanisms:

- Standard Contractual Clauses (SCCs): The European Commission has approved sets of contractual clauses that offer sufficient safeguards for personal data transfers. The SCCs impose obligations on both the data exporter and the data importer to protect the data. In June 2021, the Commission adopted new SCCs that align with the GDPR and take into account the Schrems II decision (discussed below) [40].
- Binding Corporate Rules (BCRs): BCRs are internal rules for data transfers within a multinational group of companies. They must be approved by the competent data protection authority and require significant effort to put in place [41].
- Derogations: The GDPR allows transfers based on specific derogations, such as the data subject's explicit consent, the performance of a contract, important reasons of public interest, the establishment or defense of legal claims, or the vital interests of the data subject [42].

The landscape for cross-border data transfers was significantly impacted by the Court of Justice of the European Union (CJEU)'s Schrems II decision in July 2020. The court invalidated the EU-US Privacy Shield, a framework that allowed certified US companies to receive personal data from the EU, on the grounds that US surveillance laws did not provide adequate protection for the rights of EU data subjects [43]. The court also ruled that SCCs remain valid, but organizations relying on them must assess on a case-by-case basis whether the laws of the recipient country ensure adequate protection, and provide additional safeguards if necessary [44].

As a result, organizations transferring personal data from the EU to the US (or other countries without an adequacy decision) must now conduct data transfer impact assessments, considering factors such as the nature of the data, the purpose of the processing, and the laws and practices of the recipient country. If the assessment reveals that the data would not be adequately protected,

additional measures such as encryption or pseudonymization may be necessary.

Complying with cross-border data transfer requirements in the cloud context requires close collaboration between cloud customers and providers. The allocation of responsibilities for ensuring lawful transfers should be clearly defined in contracts. Customers should understand where their data will be stored and processed, and what transfer mechanisms the cloud provider relies on. Providers should be transparent about their data handling practices and assist customers in meeting their compliance obligations.

4. Shared Responsibility Model

4.1. Division of Responsibilities

The shared responsibility model is a fundamental principle of cloud computing. It delineates the security and compliance responsibilities of the cloud provider and the customer. The exact division of responsibilities depends on the service model (IaaS, PaaS, or SaaS) and the specific services used, but the general principles are:

- The cloud provider is responsible for securing the underlying infrastructure, including the physical data centers, network, and hypervisor layer.
- The customer is responsible for securing their data, applications, and access management.
- In IaaS, the customer has the most control and responsibility, as they manage the operating systems, applications, and data. The provider is responsible for the physical infrastructure, network, and virtualization layer.
- In PaaS, the provider manages the infrastructure and the platform components, while the customer is responsible for their applications and data.
- In SaaS, the provider manages most of the stack, including the applications. The customer is primarily responsible for data and user access management.

Regardless of the service model, the customer is always responsible for classifying their data, ensuring it is handled in accordance with legal and regulatory requirements, and managing user access [45].

4.2. Implications for Compliance

The shared responsibility model has significant implications for privacy and security compliance in the cloud:

- Both the cloud provider and the customer have compliance obligations. The customer cannot fully delegate its compliance responsibilities to the provider.
- The customer must understand what controls the provider has in place and how they align with the customer's compliance requirements. This requires thorough due diligence and ongoing monitoring.
- Compliance responsibilities should be clearly defined in contracts and SLAs. The contract should specify each party's roles, the security measures the provider will implement, the customer's audit and monitoring rights, and the provider's incident response and breach notification obligations.
- The customer must implement its own security controls for the areas it is responsible for, such as data encryption, access management, and application security.
- Compliance assessments and audits should cover both the provider's and the customer's areas of responsibility. The customer should ensure it has sufficient visibility into the provider's operations to demonstrate compliance.

A key challenge is that the shared responsibility model can vary significantly between cloud providers and even between different services from the same provider. Customers must carefully review the specifics of their deployment to understand their compliance obligations.

For example, under HIPAA, a cloud provider that processes ePHI is always considered a business associate, regardless of the service model. However, the specific requirements the provider must meet, and the provisions that must be included in the BAA, will depend on the nature of the services. A provider that only offers IaaS and does not access ePHI may have more limited HIPAA obligations than a SaaS provider that directly handles ePHI [46].

Similarly, under the GDPR, both the cloud provider and the customer can be considered data controllers, joint controllers, or processors, depending on their role in determining the purposes and means of processing. The GDPR requires controllers and processors to have a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller [47]. The allocation of responsibilities between the parties must be clearly defined.

Cloud customers must also consider how the shared responsibility model impacts their ability to respond to data subject requests. For instance, if a customer receives a GDPR access request, it must be able to retrieve all the

relevant personal data, even if it is spread across multiple cloud services. This requires close coordination with cloud providers and clear procedures for handling such requests.

5. Vendor Management and Due Diligence

5.1. Vendor Risk Assessment

Engaging a cloud service provider introduces third-party risks that must be carefully managed. A robust vendor risk management program is essential for ensuring that cloud providers meet the organization's security, privacy, and compliance requirements.

The first step is conducting a thorough risk assessment of potential cloud providers. This should cover:

- Information security practices: Evaluating the provider's security controls, including physical security, network security, access controls, data encryption, and vulnerability management.
- Privacy practices: Assessing how the provider collects, uses, stores, and shares personal data, and how it complies with applicable privacy laws.
- Compliance posture: Reviewing the provider's compliance with relevant industry standards and regulations, such as ISO 27001, SOC 2, PCI DSS, HIPAA, and GDPR.
- Incident response capabilities: Evaluating the provider's incident detection, response, and notification procedures, and how they align with the customer's own incident response plan.
- Business continuity and disaster recovery: Assessing the provider's ability to maintain operations and protect customer data in the event of disruptions.
- Supply chain security: Evaluating the security practices of the provider's subcontractors and suppliers.
- Jurisdiction and data residency: Understanding where the provider stores and processes data, and how it complies with cross-border data transfer requirements.

The risk assessment should be proportional to the criticality of the data and systems being moved to the cloud. Higher-risk deployments, such as those involving sensitive personal data or mission-critical applications, require more extensive due diligence.

Organizations should leverage industry-standard questionnaires and certifications to assess cloud providers, such as the Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ) and the ISO/IEC 27017 standard for information security controls for cloud services [48].

5.2. Contractual Safeguards

Once a cloud provider has been selected, it is crucial to establish clear contractual safeguards. The contract should comprehensively address security, privacy, and compliance requirements, and provide the customer with sufficient assurances and oversight mechanisms.

Key provisions to include in cloud contracts:

- Security requirements: Specifying the security controls the provider must implement, such as encryption, access controls, logging and monitoring, and vulnerability management.
- Privacy requirements: Defining the provider's responsibilities for handling personal data in accordance with applicable laws, including data subject rights, data retention limits, and restrictions on secondary uses of data.
- Compliance obligations: Requiring the provider to comply with relevant industry standards and regulations, and to provide evidence of compliance through certifications, audit reports, or other documentation.
- Audit and monitoring rights: Giving the customer the right to audit the provider's security and privacy practices, either directly or through third-party auditors.
- Incident response and breach notification: Defining the provider's obligations for detecting, responding to, and notifying the customer of security incidents and data breaches, including specific timelines and procedures.
- Service level agreements (SLAs): Specifying the performance, availability, and reliability commitments the provider must meet, and the consequences for failing to meet them.
- Data ownership and portability: Clarifying that the customer retains ownership of its data, and requiring the provider to return or delete the data upon termination of the contract.
- Liability and indemnification: Allocating liability between the parties for security incidents, data breaches, and compliance violations, and requiring the provider to indemnify the customer for harm caused by the provider's negligence or misconduct.

Negotiating strong contractual protections can be challenging, particularly with large cloud providers that offer standardized terms of service. However, many providers are willing to negotiate custom terms for

enterprise customers, especially in regulated industries. Organizations should involve legal counsel and information security experts in the contracting process to ensure their requirements are adequately addressed.

5.3. Ongoing Monitoring

Vendor risk management does not end with the signing of the contract. Organizations must continuously monitor their cloud providers to ensure they are meeting their contractual obligations and maintaining an acceptable level of risk.

This involves:

- Reviewing security and compliance documentation: Regularly reviewing the provider's audit reports, certifications, and other documentation to verify that controls remain effective.
- Monitoring service levels: Tracking the provider's performance against SLAs and holding them accountable for any failures.
- Conducting periodic audits: Exercising audit rights to assess the provider's security and privacy practices, either through on-site assessments or remote audits.
- Monitoring incident response: Ensuring the provider is promptly detecting, responding to, and notifying the customer of security incidents and data breaches.
- Tracking regulatory developments: Staying informed of changes to applicable laws and regulations, and ensuring the provider adapts its practices accordingly.
- Managing contract changes: Documenting and approving any changes to the services or terms of the contract, and ensuring they do not introduce unacceptable risks.

Effective ongoing monitoring requires close collaboration between the organization's vendor management, information security, legal, and compliance functions. Automated tools and platforms can help streamline the monitoring process, such as continuous monitoring solutions that provide real-time visibility into the provider's security posture.

If a cloud provider is found to be non-compliant or fails to remediate identified risks, the organization should escalate the issue in accordance with its vendor management policies. In severe cases, it may be necessary to terminate the contract and transition to a new provider. Having an exit strategy and contingency plans in place is crucial for managing vendor continuity risks.

6. Incident Response and Breach Notification

6.1. Incident Response Planning

Effective incident response is critical in the cloud environment, where security incidents can rapidly escalate and spread across multiple customers. Cloud customers must have a well-defined incident response plan that covers both incidents in their own environment and incidents at their cloud providers.

Key components of a cloud incident response plan:

- Incident classification: Defining what constitutes a security incident or data breach, and establishing severity levels based on the potential impact.
- Roles and responsibilities: Identifying the individuals and teams responsible for each stage of the incident response process, including IT, information security, legal, compliance, and public relations.
- Detection and analysis: Establishing procedures for detecting, triaging, and investigating potential incidents, including gathering evidence and conducting forensic analysis.
- Containment and recovery: Defining procedures for containing the incident, mitigating its effects, and restoring systems and data to a secure state.
- Notification and communication: Establishing protocols for notifying internal stakeholders, cloud providers, regulators, and affected individuals, and for managing internal and external communications.
- Post-incident review: Conducting a formal review after each incident to identify root causes, assess the effectiveness of the response, and implement improvements to prevent future incidents.

The incident response plan should be tailored to the organization's specific cloud environment and integrated with the cloud provider's incident response procedures. This requires close coordination with the provider to ensure clear lines of communication, shared situational awareness, and a unified response.

The plan should also align with applicable legal and regulatory requirements for breach notification, such as the GDPR's 72-hour notification deadline for data controllers and the HIPAA Breach Notification Rule's 60-day notification deadline for covered entities [49] [50]. Organizations should have templates and processes in place to efficiently gather the necessary information and make the required notifications.

Cloud customers should review and test their incident response plans regularly, and conduct joint exercises

with their cloud providers to validate the effectiveness of the plans and identify areas for improvement.

6.2. Breach Notification Obligations

In the event of a data breach, organizations may have obligations to notify regulators, affected individuals, and other stakeholders. These obligations vary depending on the applicable laws and regulations, the nature and scope of the breach, and the type of data involved.

Under the GDPR, data controllers must notify the competent supervisory authority of a personal data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals [51]. If the breach is likely to result in a high risk to individuals, the controller must also notify the affected individuals without undue delay [52]. The notification must include the nature of the breach, its likely consequences, the measures taken or proposed to mitigate its effects, and the contact details of the data protection officer or other contact point [53].

Under HIPAA, covered entities must notify affected individuals, the Secretary of Health and Human Services, and in some cases the media, of a breach of unsecured protected health information. The notification must be made within 60 days of the discovery of the breach and must include a description of the breach, the types of information involved, the steps individuals should take to protect themselves, a brief description of the covered entity's investigation and mitigation efforts, and contact procedures for individuals to ask questions or learn additional information [54].

Other laws and regulations, such as the CCPA, the New York State Department of Financial Services' Cybersecurity Regulation, and sector-specific regulations like the Gramm-Leach-Bliley Act for financial institutions, have their own breach notification requirements with varying timelines and content requirements [55] [56] [57].

In the cloud context, determining whether a breach has occurred, who is responsible for making the notification, and how to coordinate the notification process can be complex. The shared responsibility model and the specific terms of the cloud contract come into play.

If a breach occurs at the cloud provider, the provider should promptly notify the customer in accordance with the contractual provisions and cooperate with the customer's investigation and response. However, the ultimate responsibility for notifying regulators and affected individuals typically remains with the customer, as the data controller.

If a breach occurs in the customer's environment, the customer should assess whether the cloud provider was involved or impacted and coordinate the response accordingly. The cloud provider may have relevant logs, forensic data, or other information that can assist in the investigation and containment of the breach.

Regardless of where the breach occurred, clear communication and coordination between the cloud customer and provider are essential for an effective response. The parties should have a joint incident response plan that defines roles, responsibilities, and communication protocols, and they should regularly test and update the plan to ensure its effectiveness.

7. Auditing and Continuous Monitoring

7.1. Auditing Requirements and Standards

Auditing and continuous monitoring are essential for ensuring that cloud environments remain secure and compliant over time. Regular audits help organizations validate that their cloud providers are meeting contractual obligations and industry standards, identify potential vulnerabilities and control weaknesses, and demonstrate compliance to regulators and other stakeholders.

Several industry standards and frameworks provide guidance on auditing cloud environments:

- SOC (System and Organization Controls) reports: SOC reports, particularly SOC 2 and SOC 3, are designed to provide assurance about a service organization's controls related to security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are intended for a restricted audience and provide detailed information about the service organization's systems and controls, while SOC 3 reports are shorter, less detailed reports intended for a general audience [58].

Copy

M

continue

- ISO/IEC 27001 and 27017: ISO/IEC 27001 is a widely recognized information security standard that specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). ISO/IEC 27017 provides additional guidance on applying ISO/IEC 27001 controls in the cloud computing context [59].

- Cloud Security Alliance (CSA) STAR: The CSA Security, Trust, Assurance, and Risk (STAR) program is a set of tools and certifications for assessing cloud providers' security posture. The CSA Cloud Controls Matrix (CCM) provides a detailed mapping of cloud-specific security controls to various industry standards, while the CSA STAR attestation and

certification programs provide independent third-party assessments of a provider's security posture [60].

- AICPA Trust Services Criteria: The American Institute of Certified Public Accountants (AICPA) has developed a set of Trust Services Criteria for evaluating the security, availability, processing integrity, confidentiality, and privacy of information systems. These criteria are used in SOC 2 and SOC 3 audits [61].

Cloud customers should require their providers to undergo regular audits against these standards and provide the resulting audit reports. The specific standards and frequency of audits will depend on the organization's risk profile, regulatory requirements, and the nature of the cloud services being used.

In addition to third-party audits, cloud customers should conduct their own periodic audits of their cloud environments. This may include reviewing the provider's security documentation, conducting vulnerability scans and penetration tests, and assessing the effectiveness of security controls and incident response procedures.

7.2. Continuous Monitoring Strategies

While periodic audits provide a point-in-time assessment of a cloud environment's security and compliance posture, continuous monitoring provides ongoing visibility and real-time detection of potential issues. Continuous monitoring is particularly important in the cloud, where the dynamic nature of the environment can introduce new risks and vulnerabilities at any time.

Key elements of a continuous monitoring strategy for cloud environments:

- Security information and event management (SIEM): SIEM tools aggregate and analyze log data from various sources across the cloud environment to detect potential security incidents and anomalies in real-time. They can help identify unauthorized access attempts, malware infections, policy violations, and other threats [62].

- Cloud security posture management (CSPM): CSPM tools continuously assess the configuration of cloud resources against best practices and compliance requirements, identifying misconfigurations, policy violations, and other risks. They can help ensure that cloud resources are provisioned securely and that configurations don't drift over time [63].

- Vulnerability scanning: Regular vulnerability scans can help identify known vulnerabilities in cloud-based systems and applications. Many cloud providers offer native vulnerability scanning tools, while third-party scanners can provide additional capabilities and coverage [64].

- Network monitoring: Monitoring network traffic and activity in the cloud environment can help detect potential security issues, such as unauthorized access attempts, data exfiltration, and denial-of-service attacks. Network monitoring tools can provide visibility into traffic patterns, protocol usage, and other indicators of compromise [65].

- Endpoint detection and response (EDR): EDR tools continuously monitor endpoints, such as servers and workstations, for signs of malicious activity. They can help detect and investigate potential security incidents, such as malware infections and unauthorized access, and provide capabilities for containment and remediation [66].

Continuous monitoring tools should be integrated with the organization's overall security operations and incident response processes. Automated alerting and remediation capabilities can help ensure that potential issues are addressed promptly, while integration with ticketing and workflow systems can help ensure that incidents are properly tracked and resolved.

Cloud providers often offer native monitoring and security tools that can provide visibility into their environments. However, customers should also consider deploying their own monitoring tools and integrating them with the provider's tools to ensure comprehensive coverage.

Effective continuous monitoring requires a combination of people, processes, and technology. Organizations should have dedicated security operations staff who are trained to use the monitoring tools and investigate potential incidents. Processes should be in place for triaging and responding to alerts, and for escalating incidents as needed. And the monitoring tools themselves should be regularly tuned and updated to ensure they remain effective as the environment evolves.

8. Evolving Considerations

8.1. Data Localization

Data localization refers to legal requirements that data be stored and processed within the borders of a particular country or jurisdiction. These requirements are often motivated by concerns about data privacy, security, and government access to data.

In recent years, there has been a growing trend towards data localization laws, particularly in the wake of the Snowden revelations about US government surveillance programs. Countries such as China, Russia, India, and several EU member states have enacted laws that require certain types of data, such as personal data or data related to critical infrastructure, to be stored and processed locally [67].

Data localization requirements can present significant challenges for cloud computing, which relies on the ability to move data seamlessly across borders. Cloud providers often operate global networks of data centers and use techniques like data replication and load balancing to ensure the availability and performance of their services.

Compliance with data localization laws may require cloud providers to segregate data geographically and ensure that data is only stored and processed in specific locations. This can be technically challenging and may require significant changes to the provider's architecture and operations.

For cloud customers, data localization requirements can limit the choice of providers and services and may impact the cost and performance of cloud deployments. Customers may need to use local or regional providers rather than global providers, and may not be able to take full advantage of the scalability and resilience of the cloud model.

When evaluating cloud providers and services, organizations should carefully consider any applicable data localization requirements and ensure that the provider can demonstrate compliance. The location of data storage and processing should be clearly specified in the service contract, along with any related security and access controls.

Organizations should also be aware that data localization laws can change over time and may vary significantly between jurisdictions. Regular monitoring of the legal landscape and ongoing communication with cloud providers is essential to ensure continued compliance.

8.2. Confidential Computing and Secure Enclaves

Confidential computing is an emerging technology that aims to protect data in use by performing computations in a hardware-based trusted execution environment (TEE), also known as a secure enclave. TEEs provide a isolated and encrypted environment for processing sensitive data, ensuring that the data remains protected even if the underlying infrastructure is compromised [68].

The main benefit of confidential computing in the cloud is that it allows customers to process sensitive data on untrusted infrastructure. Even if the cloud provider or a malicious actor gains access to the physical server, they cannot access the data being processed within the TEE.

Several major cloud providers, including Microsoft Azure, Google Cloud, and IBM Cloud, now offer confidential computing services that allow customers to run workloads in secure enclaves. These services use hardware-based technologies like Intel SGX (Software Guard Extensions) and AMD SEV (Secure Encrypted Virtualization) to create the TEEs [69].

Confidential computing can be particularly useful for scenarios involving highly sensitive data, such as:

- Multi-party computation, where multiple organizations need to process data jointly without revealing their individual inputs.
- Analytics on sensitive data, such as personal health information or financial data, where the data must be protected from unauthorized access.
- Blockchain and cryptocurrency applications, where the integrity and confidentiality of transactions must be ensured.
- Edge computing scenarios, where data is processed on untrusted devices or in untrusted environments.

To use confidential computing services, applications must be specifically designed to run in a TEE. This typically involves partitioning the application into trusted and untrusted components, and ensuring that sensitive data is only processed within the trusted component.

While confidential computing provides strong protections for data in use, it is not a silver bullet. TEEs have been shown to be vulnerable to certain types of side-channel attacks, and the security of the TEE itself ultimately depends on the underlying hardware and firmware [70].

Organizations considering the use of confidential computing services should carefully evaluate the specific offerings and their security properties. They should also ensure that their application architecture and development processes are adapted to the requirements of confidential computing.

As with any emerging technology, the legal and regulatory implications of confidential computing are still evolving. Organizations should monitor developments in this space and ensure that their use of confidential computing services is aligned with applicable laws and regulations.

9. Recommendations and Conclusion

9.1. Recommendations for Cloud Customers

To effectively navigate the complex landscape of data privacy and compliance in cloud computing, organizations should:

- Develop a comprehensive cloud governance framework that addresses data privacy, security, and compliance. The framework should define policies,

procedures, and responsibilities for managing cloud-based data and systems.

- Conduct thorough due diligence on potential cloud providers, including assessments of their security controls, privacy practices, compliance posture, and ability to meet the organization's specific requirements.
- Establish clear contractual safeguards with cloud providers, including provisions on security, privacy, compliance, auditing, and incident response.
- Implement a robust vendor management program to continuously monitor cloud providers and ensure they are meeting their contractual obligations and maintaining an acceptable level of risk.
- Develop and regularly test incident response and breach notification procedures that are tailored to the cloud environment and integrated with the cloud provider's procedures.
- Conduct regular audits and assessments of the cloud environment, using industry standards and best practices as benchmarks. Consider implementing continuous monitoring strategies to provide ongoing visibility into the environment.
- Stay informed of evolving legal and regulatory requirements, particularly in the areas of data localization and cross-border data transfers. Adapt cloud strategies and practices as needed to ensure continued compliance.
- Consider the use of emerging technologies like confidential computing to provide additional protections for sensitive data, but carefully evaluate the specific offerings and their security implications.
- Foster a culture of security and privacy awareness throughout the organization, and provide regular training to employees on their roles and responsibilities in protecting cloud-based data.
- Work collaboratively with cloud providers, industry groups, and regulators to address shared challenges and promote best practices for data privacy and compliance in the cloud.

9.2. Conclusion

Cloud computing offers significant benefits in terms of scalability, flexibility, and cost efficiency, but it also introduces complex data privacy and compliance challenges. As organizations increasingly move sensitive data and workloads to the cloud, it is critical that they understand and effectively manage the legal and regulatory risks involved.

This requires a comprehensive approach that encompasses governance, risk assessment, vendor management, contractual safeguards, incident response, auditing, and continuous monitoring. Organizations must also stay attuned to evolving legal and regulatory developments, particularly in areas like data localization and cross-border data transfers, and adapt their strategies accordingly.

Emerging technologies like confidential computing offer promising new approaches to protecting data in the cloud, but also raise new questions and challenges. As the technology and regulatory landscape continues to evolve, ongoing collaboration between cloud customers, providers, and regulators will be essential to promoting innovation while ensuring the protection of sensitive data.

Ultimately, the key to successfully navigating data privacy and compliance issues in cloud computing is to approach them proactively, systematically, and with a commitment to ongoing vigilance and improvement. By doing so, organizations can reap the benefits of the cloud while upholding their legal and ethical obligations to protect the data entrusted to them.

References

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023. (2022, October 31). Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

[2] General Data Protection Regulation (GDPR), art. 83, 2016 O.J. (L 119) 1.

[3] Cal. Civ. Code § 1798.155.

[4] General Data Protection Regulation (GDPR), art. 4(1), 2016 O.J. (L 119) 1.

[5] General Data Protection Regulation (GDPR), art. 5, 2016 O.J. (L 119) 1.

[6] General Data Protection Regulation (GDPR), arts. 12-23, 2016 O.J. (L 119) 1.

[7] General Data Protection Regulation (GDPR), art. 6, 2016 O.J. (L 119) 1.

[8] General Data Protection Regulation (GDPR), recital 32, art. 7, 2016 O.J. (L 119) 1.

[9] General Data Protection Regulation (GDPR), art. 9, 2016 O.J. (L 119) 1.

[10] European Data Protection Board. (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[11] General Data Protection Regulation (GDPR), arts. 44-50, 2016 O.J. (L 119) 1.

[12] General Data Protection Regulation (GDPR), arts. 33-34, 2016 O.J. (L 119) 1.
[13] General Data Protection Regulation (GDPR), art. 35, 2016 O.J. (L 119) 1.
[14] Cal. Civ. Code § 1798.140(c).
[15] Cal. Civ. Code §§ 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125.
[16] Cal. Civ. Code § 1798.140(o).
[17] Cal. Civ. Code § 1798.100(b).
[18] Cal. Civ. Code § 1798.110(a).
[19] Cal. Civ. Code § 1798.110(b).
[20] Cal. Civ. Code § 1798.140(t)(1).
[21] Cal. Civ. Code § 1798.185(a).
[22] Cal. Civ. Code §§ 1798.100(a)(1), 1798.121, 1798.199.10.
[23] 45 C.F.R. § 160.103 (2022).
[24] 45 C.F.R. § 160.103 (2022).
[25] 45 C.F.R. §§ 164.502-164.514 (2022).
[26] 45 C.F.R. §§ 164.302-164.318 (2022).
[27] 45 C.F.R. § 160.103 (2022).
[28] 45 C.F.R. § 164.504(e) (2022).
[29] 45 C.F.R. § 164.314(a) (2022).
[30] 45 C.F.R. § 164.314(a)(2)(i)(B) (2022).
[31] 45 C.F.R. § 164.314(a)(2)(i)(C) (2022).
[32] 45 C.F.R. § 164.504(e)(2)(ii)(H) (2022).
[33] HHS.gov. (2022, March 7). Resolution Agreements. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
[34] PCI Security Standards Council. (n.d.). About Us. https://www.pcisecuritystandards.org/about_us/
[35] PCI Security Standards Council. (2022). Payment Card Industry (PCI) Data Security Standard v4.0. https://www.pcisecuritystandards.org/documents/PCI_DSS-v4_0.pdf
[36] PCI Security Standards Council. (2018). Information Supplement: PCI SSC Cloud Computing Guidelines v3.0. https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf
[37] CLOUD Act, H.R. 4943, 115th Cong. (2018).
[38] Daskal, J. (2019). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stan. L. Rev. Online, 71, 9.
[39] European Commission. (n.d.). Adequacy decisions. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[40] European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31.
[41] European Data Protection Board. (2022). Guidelines 1/2022 on the application of Article 60 GDPR. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-12022-application-article-60-gdpr_en
[42] General Data Protection Regulation (GDPR), art. 49, 2016 O.J. (L 119) 1.
[43] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).
[44] European Data Protection Board. (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
[45] Cloud Security Alliance. (2021). Top Threats to Cloud Computing: The Egregious Eleven. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/
[46] U.S. Department of Health and Human Services. (2016). Guidance on HIPAA & Cloud Computing. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
[47] General Data Protection Regulation (GDPR), art. 28, 2016 O.J. (L 119) 1.
[48] Cloud Security Alliance. (n.d.). CSA STAR Program & Open Certification Framework. https://cloudsecurityalliance.org/star/
[49] General Data Protection Regulation (GDPR), arts. 33-34, 2016 O.J. (L 119) 1.
[50] 45 C.F.R. §§ 164.400-164.414 (2022).
[51] General Data Protection Regulation (GDPR), art. 33(1), 2016 O.J. (L 119) 1.
[52] General Data Protection Regulation (GDPR), art. 34(1), 2016 O.J. (L 119) 1.
[53] General Data Protection Regulation (GDPR), art. 33(3), 2016 O.J. (L 119) 1.
[54] 45 C.F.R. § 164.404 (2022).
[55] Cal. Civ. Code § 1798.82.
[56] 23 NYCRR 500.17 (2017).
[57] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[58] American Institute of Certified Public Accountants. (n.d.). SOC for Service Organizations. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html
[59] International Organization for Standardization. (2015). ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on

ISO/IEC 27002 for cloud services. https://www.iso.org/standard/43757.html

[60] Cloud Security Alliance. (n.d.). Security Trust Assurance and Risk (STAR). https://cloudsecurityalliance.org/star/

[61] American Institute of Certified Public Accountants. (2017). TSP Section 100: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

[62] Gartner. (n.d.). Security Information and Event Management (SIEM). https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[63] Cloud Security Alliance. (n.d.). Cloud Security Posture Management. https://cloudsecurityalliance.org/research/cloud-security-posture-management/

[64] National Institute of Standards and Technology. (2020). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[65] Center for Internet Security. (n.d.). CIS Critical Security Controls. https://www.cisecurity.org/controls/

[66] Gartner. (n.d.). Endpoint Detection and Response (EDR). https://www.gartner.com/en/information-technology/glossary/endpoint-detection-and-response-edr

[67] United Nations Conference on Trade and Development. (2021). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[68] Confidential Computing Consortium. (n.d.). Confidential Computing: Hardware-Based Trusted Execution for Applications and Data. https://confidentialcomputing.io/white-papers/

[69] Cloud Security Alliance. (2021). Confidential Computing and the Cloud. https://cloudsecurityalliance.org/artifacts/confidential-computing-and-the-cloud/

[70] Göttel, C., Pires, R., Rocha, I., Vaucher, S., Felber, P., Pasin, M., & Schiavoni, V. (2018). Security, performance and energy trade-offs of hardware-assisted memory protection mechanisms. In 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS) (pp. 133-142). IEEE.

[71] Madasu, R. "Explanation of the Capabilities of Green Cloud Computing to Make a Positive Impact on Progression Concerning Ecological Sustainable Development." Research Journal of Multidisciplinary Bulletin 2, no. 2 (2023): 5-11.

[72] Srivastav and S. Mandal, "Radars for Autonomous Driving: A Review of Deep Learning Methods and Challenges," in IEEE Access, vol. 11, pp. 97147-97168, 2023, doi: 10.1109/ACCESS.2023.3312382.

[73] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018. https://www.ijsr.in/article-description.php?id=ZU9rWnA5d3R1Q1dzK2tLSTNTbDRZZz09