Data privacy regulations require organizations — especially in regulated industries — to act ethically and responsibly with regard to personally identifiable information (PII). Selecting cloud services vendors that adhere to these laws and security requirements is essential to creating trust with customers.

Regulated Industries and Data Privacy Requirements: Act Ethically and Responsibly Regarding PII

April 2020

Written by: Adelaide O’Brien, Research Director, Government Digital Transformation Strategies

Introduction

As organizations digitally transform, CIOs and IT departments see an increasing demand for solutions that enable new, agile business models to support employee productivity, enhance customer experiences, better manage enterprise assets and resource planning, deliver appropriate services and information, and drive efficiency. Cloud is foundational to virtually all these solutions. Many agencies are launching cloud-based initiatives to help make data-driven decisions, enhance operations, and improve services.

Meeting security and compliance requirements in deploying cloud-based solutions is of paramount concern as highly regulated organizations in healthcare, financial services, and public sectors digitally transform. To begin with, there are unique data protection challenges inherent to cloud deployments, such as multiple users sharing a common IT platform and information that is shared across multiple ecosystem partners and locations. However, regulated industries are also entrusted with personally identifiable information (PII). Customers expect these industries to safeguard their personal data against those seeking to steal their identities and cause other significant personal harm.

Governments around the world are addressing the widespread availability and misuse of PII with laws and regulations to safeguard data and an individual’s privacy. Data protection and privacy by design are the core of many risk-based management decisions. Protecting data and privacy is foundational to ensure ethical actions and accountable social responsibility as well as lay strong building blocks of trust.

Three key regulations relating to data privacy and protection of personal information are the Federal Risk and Authorization Management Program (FedRAMP), the General Data Protection Regulation (GDPR), and the Cloud Computing Compliance Controls Catalogue (C5).

Federal Risk and Authorization Management Program

FedRAMP is a risk management approach comprising a standard set of approved, minimum security assessments, controls, and continuous monitoring that vendors must meet to be authorized to provide cloud services to U.S. federal agencies. FedRAMP security controls are based on NIST security baselines and contain controls above this baseline to address the unique elements of cloud computing. FedRAMP categorizes federal systems as:

» Low impact, or those meeting 125 security controls

» Moderate impact, or those meeting 325 security controls

» High impact, or those meeting 421 security controls
Federal agencies require their cloud provider to obtain FedRAMP certification due to the rigorous security checks, consistent monitoring for security vulnerabilities, end-to-end encryption of all data traffic and data at rest, government-defined architecture, and service-level agreements (SLAs). To be certified, cloud providers must also meet the requirement for United States–based personnel to support the solution.

**General Data Protection Regulation**

The GDPR governs how personal data must be collected, processed, and erased. Any organization that handles the personal information of European Union (EU) citizens or residents is subject to the GDPR. This European regulation sets out principles for the lawful processing of personal data. Processing includes the collection, organization, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure, or destruction of personal data. GDPR establishes rules on how regulated industries and other entities can process the personal data of citizens who are EU citizens or residents. GDPR requires organizations to document an effective audit trail of how and when an individual consented to give his or her data and have it used.

**Cloud Computing Compliance Controls Catalogue**

C5 is a government-backed attestation scheme introduced in Germany by the Federal Office for Information Security to assess the information security of cloud services. Similar to FedRAMP in the United States, C5 sets a baseline security level for cloud services. It aims to enable information security in a transparent way based on a standardized examination and reports. C5 leverages internationally recognized security standards such as ISO/IEC 27001 to set a consistent audit baseline that helps establish a framework of trust between cloud providers and their customers. It is intended to help organizations demonstrate operational security against common cyberattacks and adds additional controls that provide information pertaining to data location, service provisioning, place of jurisdiction, existing certification, information disclosure obligations, and a full-service description. The C5 attestation can be used by organizations and their compliance advisors to understand the range of IT security assurance services that vendors offer as they move their workloads to the cloud. Organizations can also evaluate how data privacy and their own policies or risk management posture relate to their use of cloud computing services.

**Benefits**

Using cloud services provides tremendous digital transformation opportunities, but it also involves risks. The goal of data privacy regulations is to require organizations to act ethically and responsibly with regard to PII. Selecting vendors that adhere to these laws and security requirements provides the following benefits:

- By selecting a FedRAMP-certified cloud solution, organizations can forgo the security assessment process for a multitude of known security controls, deploy a certified cloud service for their applications and workloads, and more confidently deploy systems into the certified environment.

- For both C5 and FedRAMP, certified cloud vendors are required to maintain a security authorization of continuous monitoring and ongoing security controls that meet government requirements, and they must demonstrate that the security posture of their service offering is continuously acceptable.

- GDPR requirements are designed to secure PII and make it easy for people to exercise control over their data. GDPR rebalances the relationship between individuals and organizations by enhancing the privacy rights of individuals and requiring more of organizations in terms of accountability, data protection, security, and management.
Conclusion

Employees at all levels of regulated industries must treat the personal data and information of clients and constituents confidentially and use it only to the extent permitted by law. Organizations must have visibility into their risk in selecting cloud services, and more thorough and exhaustive due diligence in selecting cloud services providers has become critically important. By understanding the sensitivity of the data, organizations in regulated industries can require the right level of security from their cloud provider. Trust is often based on whether the provider has deployed technology to protect and secure data and whether it adheres to privacy laws and regulations. Complying with legal obligations and protecting PII are essential factors in creating a relationship of trust with those served.

About the Analyst

Adelaide O’Brien, Research Director, Government Digital Transformation Strategies

Adelaide O’Brien is a dedicated government analyst who understands agency requirements and mandates and has deep technical expertise in analytics, AI, and cloud. She has been recognized as a valued thought leader by U.S. federal agencies and the vendors serving government and named one of the top 100 leaders from throughout the federal IT community.
MESSAGE FROM THE SPONSOR

Organizations of every size and type are embracing digital transformation. But public sector agencies and businesses in highly regulated industries face unique challenges along the way. With one platform, agencies can modernize citizen, customer and employee experiences, streamline processes and empower employees. Get the tools you need to accelerate your digital transformation and drive new levels of insights and innovation.

The content in this paper was adapted from existing IDC research published on www.idc.com.