Data Privacy Law

9th March 2026



Idorenyin Ekpenyong [1]

Beyond The Law: Why Data Privacy Lawyers Must Understand Cloud Data Storage

Introduction

Organizations around the world depend on digital systems to collect and process personal information of employees, customers, and vendors. Over time, much of this information has migrated from traditional on-site infrastructure to cloud-based systems, changing the methods by which personal data is stored, managed, and transmitted across jurisdictions. Cloud platforms allow organizations to store and manage large volumes of personal data while benefiting from key advantages such as scalability, remote accessibility, and cost efficiency. Businesses can expand storage capacity as needed, support collaboration across multiple locations, and maintain continuity of operations without relying heavily on physical IT infrastructure. These benefits have accelerated the adoption of cloud services across industries.[2]

However, the use of cloud technologies also introduces complex legal and regulatory considerations. Issues relating to data jurisdiction, information security, third-party processing, and cross-border data transfers often arise because cloud infrastructure is typically distributed across multiple geographic locations and managed by external service providers. As a result, organizations must carefully evaluate how personal data is stored, accessed, and protected within these environments in order to comply with applicable data protection obligations.

In this context, data privacy lawyers must develop at least a foundational understanding of how data is stored and managed in cloud environments. Such knowledge enables them to better interpret regulatory requirements, identify potential risks, and provide more practical

---

[1] **Idorenyin Ekpenyong, Associate,** Intellectual Property and Technology Department, S.P.A. Ajibade & Co., Lagos, Nigeria.

[2] Oracle, 'The Benefits of Cloud Storage' available at <https://www.ibm.com/think/topics/cloud-storage> assessed on March 7th, 2026.

legal and compliance guidance to organizations operating in an increasingly cloud-driven digital ecosystem.

1. How Cloud Data Storage Works[3]

Cloud data storage operates by hosting information on remote servers managed by cloud service providers rather than on local devices controlled by the organization. These servers are located in data centers that may be distributed across multiple geographic regions, allowing organizations to upload data and access it remotely via the internet. Unlike traditional storage on a single physical server, cloud storage uses distributed architectures where data can be segmented and replicated across multiple servers to improve reliability, performance, and disaster recovery. This means personal data may exist in several locations simultaneously so that it remains available even if one server or data center fails.

To protect stored information, cloud providers implement security and storage management mechanisms such as encryption, access controls, and redundancy. Encryption converts data into a format that cannot be read without a decryption key, safeguarding confidentiality. Access controls determine who is authorized to view or modify data, while redundancy achieved through data replication ensures copies of information remain available if the primary storage location becomes unavailable. These technical measures help maintain data integrity and security within cloud environments while supporting continuous accessibility for authorized users.

From a compliance perspective, these technical characteristics of cloud storage have legal implications. Because data may be stored in different jurisdictions and managed by third-party providers, organizations must understand how cloud systems operate in order to address regulatory obligations relating to data protection, security, and cross-border transfers. A foundational understanding of cloud storage mechanisms therefore enables privacy lawyers to provide more informed advice and support effective data governance practices.[4]

2. Why Data Privacy Lawyers Must Understand Cloud Data Storage

Data privacy lawyers must understand cloud data storage because personal data is increasingly processed and stored in distributed cloud environments rather than traditional on-premise systems. Cloud storage affects legal obligations relating to data security, jurisdiction, and regulatory compliance, as information may be replicated across multiple locations and managed by third-party providers. Without a practical

---

[3] Google Cloud, 'What is Cloud Storage?' available at <https://cloud.google.com/learn/what-is-cloud-storage> accessed on March 7th, 2026.

[4] IBM, 'What is Cloud Storage?' available at <https://www.ibm.com/think/topics/cloud-storage> accessed on March 7th, 2026.

appreciation of how cloud systems operate, how data is stored, accessed, and protected, privacy lawyers may struggle to assess risks, interpret compliance requirements, and provide meaningful legal guidance. Understanding cloud storage therefore enables lawyers to bridge the gap between legal principles and technological realities in modern data governance.

2.1 High Reliance on Cloud Infrastructure

Organizations across industries increasingly rely on cloud service providers to host critical data and business applications. This shift means that personal data is often stored in distributed data centers rather than on local servers controlled directly by the organization. As a result, privacy lawyers must understand the operational model of cloud services in order to properly assess compliance obligations and potential risks.

In many cloud environments, data is not stored in a single fixed location but is distributed across multiple data centers, sometimes located in different jurisdictions. Cloud providers often replicate and distribute data across their infrastructure to ensure system resilience, backup integrity, and high availability. While these mechanisms improve operational efficiency and reliability, they can also complicate an organization's ability to determine precisely where personal data resides at any given time.

For privacy lawyers, this technical reality introduces new compliance challenges. Data protection laws frequently impose obligations related to data localization, cross-border transfers, and accountability for third-party processing. If personal data is replicated across several servers or moved between regions by a cloud provider, organizations must still ensure that such transfers comply with applicable regulatory requirements. Without an understanding of how cloud service providers structure their storage architecture and manage data flows, it becomes difficult for legal professionals to accurately assess whether an organization's practices align with these legal obligations.

2.2 The Legal Implications of Cloud Data Storage

Cloud storage raises several legal questions relating to data protection obligations, including determining the roles of controllers and processors, contractual responsibilities with cloud providers, and the allocation of liability in the event of a data breach. Without an understanding of how cloud storage operates, privacy professionals may struggle to properly interpret these legal relationships.

One of the primary legal issues arising from cloud storage is the determination of the roles of data controllers and data processors. In many cases, the organization that collects personal data will act as the data controller, while the cloud service provider functions as a processor that stores or processes the data on the controller's behalf.

However, this distinction is not always straightforward. Certain cloud providers may exercise a degree of control over how data is handled, particularly where they determine aspects of data processing or use the data for service improvement or analytics. Privacy lawyers must therefore understand the operational structure of cloud services in order to correctly determine whether a provider is acting purely as a processor or whether elements of joint controllership may arise.

Furthermore, privacy lawyers must consider the regulatory implications of outsourced data storage, particularly where cloud providers rely on subcontractors or secondary service providers. Many cloud infrastructures involve multiple layers of sub-processing, which can complicate regulatory compliance, vendor oversight, and audit obligations. Privacy lawyers must therefore be able to evaluate whether appropriate safeguards are in place and whether organizations retain sufficient oversight over how personal data is processed within the cloud ecosystem.

2.3 Cross-Border Data Transfers and Jurisdictional Issues

Cloud infrastructure frequently involves the storage or processing of data across multiple jurisdictions. This can create complex compliance challenges, particularly where privacy laws impose restrictions on international data transfers. Lawyers must therefore understand where data is physically stored and how cloud providers manage global data flows.

One of the primary challenges arises from the fact that many data protection laws impose restrictions on the transfer of personal data outside the jurisdiction in which it was originally collected. These laws are designed to ensure that personal data remains protected even when it moves across national borders. For example, the NDPA[5] prohibits transferring personal data outside the Nigeria unless the destination country offers an adequate level of protection[6] or appropriate legal safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) are in place to ensure that the data remains protected according to Nigerian standards. This requirement applies even when a cloud provider is technically secure, because the legal framework governing the data must be maintained across jurisdictions. Failure to meet these transfer conditions can result in significant enforcement actions and compliance liabilities for organizations relying on cloud infrastructure for global data flows[7].

---

[5] Section 41-42, *Nigeria Data Protection Act*, (NDPA) 2023.
[6] Schedule 5, *General Application and Implementation Directives* (NDPA - GAID) 2025.
[7] Section 48(1) Nigeria Data Protection Act, 2023,
Templars, 'Navigating the Enforcement Framework under the Data Protection Act 2023' available at <https://www.templars-law.com/app/uploads/2023/11/Navigating-the-Enforcement-Framework-under-the-Data-Protection-Act-2023.pdf> accessed on April 2nd, 2026.

Jurisdictional issues can also arise in relation to government access to data. Where personal data is stored in a particular country, it may become subject to the laws and regulatory powers of that jurisdiction, including lawful access requests by public authorities. In some cases, cloud providers may also be required to comply with the laws of the country in which they are headquartered, even if the data itself is stored elsewhere. These overlapping legal regimes can create uncertainty regarding which laws apply and how organizations should respond to regulatory or law enforcement requests.[8]

Given these complexities, privacy lawyers must develop an understanding of how cloud infrastructure manages global data flows. This knowledge enables them to conduct proper due diligence on cloud providers, advise organizations on appropriate transfer safeguards, and ensure that cross-border data processing activities remain compliant with applicable data protection laws.

2.4 Shared Security Responsibilities in Cloud Environments.

Cloud computing operates under a “shared responsibility model,” where both the cloud provider and the customer share responsibility for protecting data. Understanding this model helps privacy lawyers assess whether appropriate security safeguards are in place and whether organizations are meeting their regulatory obligations.[9]

Under this framework, the cloud provider is generally responsible for the security of the cloud, which includes protecting the underlying infrastructure such as physical data centers, servers, networking systems, and core cloud platforms. These providers invest heavily in securing their environments through advanced monitoring systems, physical security controls, and infrastructure-level protections designed to safeguard the stability and integrity of their services.

On the other hand, the organization using the cloud service is typically responsible for the security of what it places in the cloud. This includes managing access controls, configuring security settings, protecting user credentials, implementing encryption where necessary, and ensuring that personal data is properly managed within the cloud environment. In many cases, data breaches involving cloud systems occur not because the cloud infrastructure itself was compromised, but because of

---

8 Tope Adebayo LP, ‘Moving Personal Data across Borders? What Your Startup Needs to Know’ available at <https://www.mondaq.com/nigeria/data-protection/1729096/> accessed on March 7th 2026.

9 John Eustice, Miller & Chevalier, ‘Understanding cloud data protection and data privacy' available at <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> accessed on March 7th 2026.

misconfigurations, weak access management, or inadequate internal security practices by the customer organization.[10]

For privacy lawyers, understanding this shared responsibility model is critical when evaluating whether an organization has implemented appropriate technical and organizational measures to protect personal data, as required by many data protection laws. Without a clear appreciation of how responsibilities are divided between the cloud provider and the customer, it may be difficult to determine where accountability lies in the event of a security incident or data breach.

2.5 Vendor Risk Management and Contractual Safeguards.

The use of cloud services introduces third-party risk because organizations rely on external providers to store and process personal data. This reliance makes vendor risk management a core element of data protection compliance, and privacy lawyers play an important role in ensuring that contractual safeguards regulate how cloud providers handle personal information. Without appropriate agreements and oversight, organizations may face compliance and security risks arising from the actions or omissions of third-party service providers.

A key component of vendor risk management is the review and negotiation of data processing agreements between the organization and the cloud provider. Data protection laws generally require that when a data controller engages a processor, the relationship be governed by a written contract that clearly defines the processor's obligations[11]. These agreements should outline the scope and purpose of processing, the categories of personal data involved, the duration of processing, and the respective responsibilities of both parties in safeguarding the data and ensuring compliance with applicable regulations.[12]

Privacy lawyers must also assess security commitments, incident response obligations, and sub-processor arrangements within cloud contracts. Contracts should address issues such as encryption, access controls, and monitoring measures to ensure adequate security safeguards. They must also define procedures for incident notification and cooperation in the event of a data breach, as organisations often face strict regulatory reporting requirements**.** In addition, privacy lawyers should carefully review indemnity clauses, limitations of liability, and exclusions to ensure that risks arising from data breaches, regulatory non-compliance, service failures, or

---

[10] Cloudian, 'Data Security in Cloud Computing: Who Is Responsible?' available at <https://cloudian.com/guides/data-security/data-security-in-cloud-computing-who-is-responsible/> accessed on March 7th 2026.

[11] Article 34, General Application and Implementation Directives (NDPA - GAID) 2025.

[12] Trust Arc, 'Vendor Risk Management for Privacy Programs: How to Streamline Third-Party Risk and Strengthen Compliance' available at, <https://trustarc.com/resource/vendor-risk-management-privacy- >accessed on March 7th 2026.

unauthorised processing are appropriately allocated between the parties. Where cloud providers rely on sub-processors, contractual provisions should ensure transparency and impose equivalent data protection obligations on downstream service providers to maintain compliance and data security throughout the processing chain.

2.6 Bridging the Gap between Law and Technology

Privacy lawyers are required to translate regulatory obligations into practical controls that can be implemented within digital systems. For example, legal principles such as data minimization, purpose limitation, and storage limitation must be reflected in how data is structured, stored, accessed, and retained within cloud platforms. Without a working understanding of these technological environments, it becomes difficult for legal professionals to ensure that privacy obligations are effectively operationalized.

This evolving role also requires privacy lawyers to collaborate closely with multidisciplinary teams, including IT professionals, cybersecurity specialists, cloud architects, and governance personnel. These teams are responsible for designing and maintaining the systems that handle organizational data, while privacy lawyers provide the legal guidance needed to ensure that such systems comply with applicable data protection frameworks. Effective communication between these disciplines is essential for identifying potential risks early and embedding privacy considerations into system designs and operational processes.

3. Conclusion

The growing use of cloud technologies has expanded the scope of data privacy compliance beyond traditional legal analysis. Privacy professionals must understand how data is stored, processed, and secured in cloud systems in order to offer practical guidance, identify potential regulatory risks, and help organizations establish strong data governance practices. As privacy regulation increasingly intersects with technological infrastructure, legal and privacy practitioners benefit from developing an awareness of how cloud architectures operate, including data distribution, security controls, and the responsibilities of service providers, so that compliance strategies reflect real-world operational realities. Understanding how cloud storage works including data distribution, security configurations, and vendor responsibilities enables legal professionals to better interpret regulatory requirements and assess how those requirements apply in real-world operational settings.[13]

---

[13] New Zealand Law Society, 'Cloud Computing Guidelines for Lawyers' available at <https://www.lawsociety.org.nz/professional-practice/practice-briefings/cloud-computing-guidelines-for-lawyers> accessed on March 7th 2026.

Such knowledge also allows privacy lawyers to anticipate potential compliance risks, particularly in areas such as cross-border data transfers, vendor management, and cloud security practices. By appreciating how cloud providers structure their services and manage data flows, lawyers are better positioned to identify vulnerabilities, ask the right questions during due diligence, and ensure that contractual safeguards adequately protect personal data.

By understanding how data is stored, managed, and protected in cloud environments, privacy lawyers can provide more practical guidance, support stronger compliance frameworks, and help organizations navigate the growing regulatory expectations surrounding the protection of personal data.

For further information on this article and the area of law,
please contact **Idorenyin Ekpenyong**
at S. P. A. Ajibade & Co., Lagos by
Telephone (+234 814 594 2221; +234.811 890 3060; +234.806 437 3384)
Mobile (+2347038229780)
Email: iekpenyong@spaajibade.com
www.spaajibade.com