Integrating Global Privacy Frameworks in Cross-Border Financial Institutions

Olusoji Alebiosu, Adeyinka Victor Adebayo

Olabisi Onabanjo University, Ago-Iwoye, Iwoye, Ogun State, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2025.100800028

Received: 28 July 2025; Accepted: 02 August 2025; Published: 01 September 2025

ABSTRACT

In an increasingly data-driven global economy, cross-border financial institutions face mounting challenges in aligning diverse data privacy regulations across jurisdictions. This paper investigates the complexities of integrating global privacy frameworks, with a comparative focus on the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Nigerian Data Protection Regulation. By analysing the legal, operational, and technological implications of these regimes, the study explores how regulatory divergence impacts financial institutions' compliance strategies, data governance practices, and cross-border service delivery. Through an in-depth review of legal mechanisms for data transfer, case studies from Europe, the United States, and Nigeria, as well as an examination of the role of cloud computing, the paper reveals the tensions between regulatory compliance, innovation, and operational efficiency. Emphasising the need for harmonisation, it proposes integrated compliance frameworks, privacy-by-design principles, and the adoption of artificial intelligence as enablers of regulatory agility. The findings underscore the importance of international cooperation and adaptive policy design in fostering resilient, privacy-compliant financial ecosystems.

Keywords: Data privacy, Cross-border financial institutions, GDPR, CCPA, Nigerian Data Protection Regulation, Cloud computing,

INTRODUCTION

Data and information are valuable assets for financial institutions. Managing, processing, and transmitting these assets is crucial, as they may contain confidential information related to the institution or its customers. As a result, implementing appropriate controls to protect the confidentiality, integrity and availability of these assets is essential. This is where information security comes in: a practice designed to protect an organisation's assets. Privacy refers to an individual's freedom to determine the conditions under which they share information about him or herself. General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and Nigeria Data Protection Regulation (NDPR) are considered the latest and most significant developments on the data protection arena, especially for the financial sector, because of the frequency of cross-border transactions made by clients and the constant moving of client's files (Ramos & Solana, 2020). The global financial crisis has revealed a series of shortcomings in market practices and regulations. While recent developments in new bank resolution frameworks tend to address such shortcomings, they create significant tensions with insolvency law principles. The first part of this paper analysed this tension and explored three main issues: the group dimension, crisis-prevention and crisis-management tools and the cross-border dimension. This second part focuses on the cross-border dimension, exploring policies, principles, applicable law, mutual recognition, and cooperation. A critical analysis of cross-border resolution frameworks reveals several unresolved issues and uncertainties resulting from frictions between conflicting principles and policies (Kalogiannidis, 2024)

OVERVIEW OF GLOBAL PRIVACY FRAMEWORKS

Global privacy frameworks are essential for safeguarding personal information during international data transfers. The absence of a worldwide standard governing cross-border data flows complicates the financial services sector. Institutions must navigate the discrepancies among regulations while also recognising that compliant frameworks are essential for operating in multiple jurisdictions. Institutions that integrate global

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

standards with local regulations throughout their organisations benefit from an efficient and consistent resolution for data exchange transactions. In recent years, numerous countries have enacted comprehensive data protection legislation, presenting challenges to implementing and maintaining efficient accountability and risk management programs. Nonetheless, a growing body of laws permits the collection and movement of personal information—for example, the European model, developed around individuals' data-protection rights, and the U.S. approach, focused on sectoral procedural rules. A range of global and standard-setting instruments creates a framework that, if applied, can bridge these approaches (Ramos & Solana, 2020). Among the most prevalent are the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and Cross-Border Privacy Rules (CBPR), the Generally Accepted Privacy Principles (GAPP) of the American Institute of Certified Public Accountants, and the EU-U.S. Privacy Shield. Although these frameworks generally require organisations to provide individuals with transparent data-collection practices, they vary in the extent of compliance necessary (Fiero & Beier, 2022). Indeed, the difficulty in identifying a coherent framework that integrates all known sets of standards is compounded by the absence of a common regulatory language or reporting structure. Even well-developed frameworks differ in ways that make unambiguous comparisons or applications problematic. However, instituting and maintaining an organisation-wide respect for data protection remains a path to effective and timely compliance with pending legislation. (Babikian, 2023)

2.1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a European privacy standard that was published in 2016 and took effect on 25 May 2018, replacing the Data Protection Directive 95/46/EC. It applies to any personal data concerning individuals within the EU and shapes the interaction of all companies handling EU data (Maria Lopes & Oliveira, 2018). The definition of personal data is broad, encompassing any information related to an individual that directly, indirectly, or in combination with additional information allows for identification. Identifiers include names, online identifiers, passport numbers, physical addresses, and data linked to physical, physiological, genetic, mental, economic, cultural, or social identity. The inclusion of third parties mentioned in emails as personal data highlights the regulation's extensive reach. The regulation ensures a uniform basic level of protection for personal data across all EU member states and grants rights such as the right to be forgotten and data portability. It introduces the roles of data processor and Data Protection Officer, requires risk analyses and documentation of processing operations, mandates reporting security breaches to national authorities, and calls for informing data subjects using standardised icons. Sanctions are strictly prescribed in cases of non-compliance, and the 'One-stop-shop' mechanism simplifies processes involving multiple member states. Sensitive categories of personal data, including health information, receive special protection (Sirur et al., 2018).

2.2. California Consumer Privacy Act (CCPA)

Legislation addressing the personal information of California residents falls under the California Consumer Privacy Act (CCPA) (Birrell et al., 2023). The CCPA went into effect on January 1, 2020, and applies to certain for-profit entities that collect personal information from California residents and meet one or more specified thresholds. The act defines personal information broadly and establishes 11 categories, including identifiers, biometric data, internet activity, geolocation, and employment information. Data subjects have several rights, including access, deletion, the right to opt out of the sale of their personal information, the right to nondiscrimination, and data portability. The act imposes various obligations on businesses, including notice and transparency requirements, purpose limitations, security measures, record-keeping requirements, and prohibitions on discrimination. The California Privacy Rights Act (CPRA) amends the CCPA, with an effective date of 1 January 2023 (Samarin et al., 2023).

2.3. Nigerian Data Protection Regulation

An overarching Nigerian data protection law comparable to South Africa's Protection of Personal Information Act or the EU's General Data Protection Regulation is absent (Akindele, 2017). The closest instrument is the Draft Guidelines on Data Protection, developed by the National Information Technology Development Agency, which differs in that it is a soft code without specific mandatory provisions. Section 37 of the Nigerian Constitution guarantees the right to privacy only for Nigerian citizens, as it relates to the enforcement of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

fundamental human rights. The guarantee is not extended to non-citizens, where Section 45 classifies the right as neither fundamental nor absolute. Nigeria has been assessed as having no privacy law. In circumstances where Nigerian data protection law is currently at a constitutional level with limited enforcement, legal uncertainty persists regarding the protection of personal data processed or transferred to Nigeria, despite the right to privacy being an established constitutional freedom for Nigerian nationals.

CROSS-BORDER DATA TRANSFERS

Cross-border transfer is at the core of provisions addressing transboundary data flows (D. Mitchell & Hepburn, 2018). A transfer may take the form of a mere transmission, without further processing, or may also include complex processing of the data at the destination. Several regimes recognise the possibility of transboundary flows and regulate the transfer by imposing conditions of varying stringency. Schemes that conceive of transfer as processing give a more central role to transborder data flows. In these circumstances, transfer takes place if the controller sends data to another controller or processor located outside the jurisdiction, or if the controller carries out an operation that implicates a "making available" to a third party located abroad—an example being uploading to a cloud service (Pearce & Platten, 1998). In some cases, the jurisdictions of the initial transmission from the controller or processor and the subsequent processing operation may differ. For example, the controller may be located in Silicon Valley, with an intermediate processor in Virginia and an entity managing a cloud service in Madrid. When the data are transmitted from the processor to the cloud, a new "transfer" occurs, potentially subject to additional requirements.

3.1. Legal Mechanisms for Data Transfers

The European Directive on Data Protection outlines the mechanisms governing the transfer of personal data to third countries in the absence of a Commission adequacy decision. The principal mechanism involves an international agreement between the exporting and importing countries. Such agreements must be authorised by the Commission and provide adequate safeguards that cover data subjects' rights and freedoms, the transfer procedures and purposes, and proper supervision (Pearce & Platten, 1998). In the absence of such international agreements, data transfers are permissible if the data controller stipulates adequate safeguards, furnished by a contract between an organisation established in the European Economic Area and a counterpart established in the territory of a third country. The contract must specify the recipient's commitments to respect the rights and freedoms of data subjects, the conditions for data transfer, and the arrangements for supervision. Contracts are a practical alternative when no adequacy decision exists and negotiations of international agreements would require more time. Other derogations include situations where the data subject has explicitly consented; contracts between the data subject and the controller or between the controller and a third party in the data subject's legitimate interests; protection of the vital interests of the data subject; and transfers from registers intended by law for public consultation. Additional derogations address situations where the transfer is of national security interest, involves legal proceedings, or is necessary for the establishment, exercise, or defence of legal claims. Cross-border contracts, highly relevant in the financial sector, arise in specific types of transactions such as consumer contracts or human resource management (Corley, 2016). Implementation of the Directive is entrusted to a supervisory body vested with investigative and collective powers, capable of recommending or imposing corrective measures. (Marelli, 2024)

3.2. Challenges in Cross-Border Data Compliance

The integration of Corporate Privacy Policies and Binding Corporate Rules (BCR), as initially conceived within the European context, can be extended to cross-border financial institutions operating in the Asia-Pacific (APAC) region. Implementing these policies is straightforward for large financial groups that have established dedicated global compliance departments—such as Barclays, OCBC, or Standard Chartered—which oversee the global compliance framework and provide harmonised guidance to local entities based on global standards and local regulations. In contrast, financial institutions with a local focus confront greater challenges because they lack the resources or critical mass to adopt these integrated global policies. Moreover, with multiple countries and territories involved, financial institutions must choose the appropriate data transfer mechanism applicable to the region, whether BCR or the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system. The sustainability of these mechanisms now becomes crucial in preventing the proliferation of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

independent frameworks that create widespread non-compliance (Vil, 2010; Kulesza, 2012).

COMPARATIVE ANALYSIS OF GDPR, CCPA, AND NIGERIAN DATA PROTECTION REGULATION

Many privacy-by-design schemes have been proposed to assist software developers with implementing the increasing number of ever-changing privacy requirements. However, there is no universal scheme that can address all privacy requirements a developer would need to implement. As emerging privacy laws, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Nigerian Data Protection Regulation, continue to evolve, aligning these requirements with resilience must be considered, as it enhances software availability and reliability. This paper investigates the intersection of eight privacy-by-design schemes and privacy laws in addressing privacy requirements, specifically the GDPR (Europe), CCPA (US), and Nigeria Data Protection Regulation (Africa), and discusses how each scheme can support resilience in meeting these obligations. This paper provides a comparative high-level overview of three privacy regulations: the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Nigerian Data Protection Regulation. A comparison is necessary because disparities exist across these three regulations, and developers are often required to implement a system that adheres to two or more of these regulations (Aljeraisy et al., 2022). Substantial disparities exist in the protection afforded by these regulations. The growing requirement for compliance with these regulations necessitated clarity in understanding the terms and mapping the policy rules to the requirements of these regulations. Reflecting this, a high-level, nuanced comparison of some notable sectors under the three data protection laws is presented.

4.1. Key Similarities

Most global privacy frameworks follow a similar logic in guiding organisations. Their high-level principles can generally be distilled into four categories. First, they establish criteria regarding the origins of personal data and the conditions for legal collection. Second, they determine how personal data should be stored and the measures necessary to ensure its confidentiality and security. Third, they outline the rights individuals retain over their collected data. Finally, they specify the obligations imposed upon organisations that collect and store personal data. The Integrated Compliance Framework enables companies to efficiently meet their compliance needs by defining regulatory requirements and providing a suitable vocabulary for incorporating these requirements into applications (Vil, 2010). For example, suppose a company collects a customer's name and credit card number for a payment. In that case, the European Data Protection Directive requires that the name can be stored indefinitely, while the credit card number must be deleted once the transaction is finalized.

4.2. Key Differences Affecting Financial Institutions

Cloud computing has gained interest for reducing costs, offering flexible demand, and providing access to specialised servers, such as GPGPU (Vil, 2010). Frameworks like the NIST Cloud Computing Reference Architecture define five key roles: consumer, provider, carrier, broker, and auditor, each with distinct functions and responsibilities. The widespread use of virtual resources complicates monitoring resource behaviour, as higher utilisation boosts efficiency but can hide malicious activities. Financial institutions face regulatory complexities, with non-compliance posing significant risks to their financial stability and operational integrity. Divergent legal standards across regions, primarily those of the US and Europe, hinder international data cooperation. As data becomes critical for regulation and transparency, global harmonisation and new cooperation strategies are essential.

Category	Key Differences/Challenges	Impact on Financial Institutions
Cost and Efficiency	Cloud offers reduced costs and scalable resources (e.g., GPGPU access)	Enables flexible IT spending but raises challenges in ensuring secure and compliant scaling
Cloud Roles & Ecosystem	NIST defines five roles: consumer, provider, carrier, broker, and auditor	Complex interactions and shared responsibility models increase operational and compliance overhead

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Resource Monitoring	Virtualisation and multiplexing make behaviour tracking difficult	Increases difficulty in detecting security breaches or unauthorised access
Security Risks	High utilisation can conceal malicious activity.	Financial institutions face increased exposure to cyber threats and data breaches
Regulatory Compliance	Diverse and region-specific legal requirements (e.g., US vs EU privacy laws)	Compliance becomes costly and time-consuming; missteps may lead to fines and reputational damage
Governance Complexity	Weak or inconsistent global regulation frameworks	Limits cross-border operations and integration with global cloud services
Transparency and Auditability	Limited visibility into cloud provider infrastructure and processes	Makes it more challenging to satisfy regulators and internal audit requirements
Data Sovereignty	Conflicting national laws on data protection and storage locations	Institutions must navigate legal minefields when storing or processing customer data abroad
Operational Risk	Shared cloud environments introduce new vulnerabilities	Institutions must enhance risk management frameworks to address novel threats
International Cooperation	Lack of harmonised data and privacy laws across countries	Inhibits global regulatory collaboration and uniform compliance strategies

CASE STUDIES OF FINANCIAL INSTITUTIONS

This section highlights examples of cross-border financial institutions facing challenges in balancing financial service provision with data privacy and regulatory compliance. The industry is key to global economic growth and is regulated to protect market stability. Providing affordable services is a priority; however, current systems often fail to meet international needs. While better policies can address risks, social, cultural, and resource factors complicate efforts. Regulation vs. innovation tensions can disadvantage vulnerable or excluded customers. Many innovative services depend on sensitive data to improve risk assessment and customise offerings, but balancing this with regulations like the EU GDPR is complex:

“In particular, using loan-history data from social media to develop risk-scoring algorithms has raised concerns that current regulations have not caught up with Big Data analytics, highlighting the risks of safeguarding data privacy. More generally, the challenges posed by ‘Know Your Customer ‘and ‘Anti-money Laundering ‘requirements create tension for financial institutions that seek to understand and assist vulnerable customers, leading to ‘a catch-22 problem: the more data analysts obscure the digital breadcrumbs of customers online, the less well the financial institutions can know and help them’” (Elliott et al., 2021). Addressing this requires collaboration among financial institutions, regulators, and citizen representatives. Without strong regulatory support, especially for vulnerable customers, innovation may be hindered by industry risk aversion.

5.1. Case Study: European Financial Institution

Consider a financial institution based in the European Union that is subject to the European Union's General Data Protection Regulation (GDPR). Serving an international clientele, the institution must transmit and, at times, store the same data in accordance with over twenty national privacy laws and sector-specific regulations, including the American Health Insurance Portability and Accountability Act (HIPAA) and Canadian confidentiality standards, which are among the most pertinent examples. Divergent perspectives on privacy and data protection can introduce complexities, potentially resulting in non-standard behaviours (Coley, 2017).

5.2. Case Study: US-Based Financial Institution

A financial services company experiencing significant growth through acquisitions integrates third-party applications to realise operational efficiencies and establish a common platform for future enhancements. The

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

need to audit compliance creates challenges for information technology and legal managers, hindering the rapid development and timely delivery of services. An integrated compliance framework enables the organisation to construct layered mechanisms aligned with sector regulations and corporate governance. It provides an audit trail for comprehensive process and compliance documentation, while allowing for rapid application development with embedded compliance adherence. The limited mature case law on privacy frameworks and individuals' inclination to litigate to protect their information places the responsibility on institutions to understand and abide by a multitude of regulations and codes of conduct, especially concerning the processing of financial data (Vil, 2010).

5.3. Case Study: Nigerian Financial Institution

Anonymisation (differential privacy, K-anonymity, T-closeness, L-diversity) and cryptography (homomorphic encryption, private set intersection, proxy re-encryption, secure multi-party computation, zero-knowledge proofs) can support legal challenges; however, the existence of legal requirements often renders them inapplicable for core real-time payment flows. Although these requirements have been implemented, fine-grained control of encrypted data remains a challenge, particularly for downstream actors. The constitutive effect of regulations on data subjects, such as the requirement for explicit consent, creates a contradictory environment that compromises the efficacy and enforceability of the law. For cross-border financial institutions, a global framework that accommodates the diversity and volume of privacy regulations has become mandatory (Elliott et al., 2021).

REGULATORY COMPLIANCE STRATEGIES

Cross-border financial institutions frequently face legal obligations to monitor and disclose transactions to government agencies while maintaining the confidentiality of such information. Under these circumstances, regulations concerning the global privacy of financial data may conflict with AML or counterterrorism initiatives (A. de Dios, 2016). To create a more comprehensive legislation protecting the privacy of financial expenditures, a new regulatory pillar can be integrated with existing AML requirements. This sixth pillar mandates that Chief Compliance Officers within financial institutions appoint or collaborate with privacy and security specialists responsible for continuously assessing the compliance program for risks and inadequacies. These privacy professionals enhance transparency and prevent the overextension of compliance measures beyond legal mandates, particularly those related to AML. Furthermore, privacy specialists must coordinate closely with other compliance teams to maintain consistent safeguards across all service providers, addressing the extraterritorial nature of financial data. Given the absence of international harmonisation between AML and privacy regulations, FinCEN can bolster its AML framework by instituting this sixth pillar, obliging financial institutions to engage privacy experts who are charged with auditing programs, developing additional safeguards, and maintaining vigilant oversight of both AML and privacy concerns.

6.1. Developing a Compliance Framework

The growing need for an integrated, coherent compliance framework stems from the regulatory processes that continually evolve in response to accelerating technological development (Vil, 2010). Regulators acknowledge the difficulties of multiple frameworks, which impose costly and potentially conflicting requirements on organisations operating in geographically diverse and sectorally diversified markets. Thus, an attractive approach involves integrating existing regimes and applying them as a unified global framework. Cross-border financial institutions are subject to the jurisdiction of multiple national data protection laws and regulations. Several institutions have already expressed ambitions to comply with various regulatory requirements. However, no comprehensive compliance framework currently incorporates different regimes into a systematic framework tailored to the characteristics of these entities, addressing the inevitable overlaps and inconsistencies. Such a proposal offers a higher level of security for financial customers and facilitates dealing with regulators and other institutions.

6.2. Monitoring and Auditing of Training and Awareness Programs' Compliance

Training and awareness programs must be conducted regularly for all employees and end-users to understand

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

the policies and standards of the Privacy Governance Framework, particularly their responsibilities when processing the personal data of customers and other stakeholders. Highly targeted technical awareness programs are also recommended for data custodians and data processors based on their responsibilities and the nature of systems being managed. Key initiators for these programs include the various direct and indirect risks that affect the institution's processes, applicable legal and regulatory requirements, overall governance drivers, and the financial institution's internal control framework. The ever-changing nature of privacy regulations worldwide presents significant challenges for cross-border financial institutions, such as private banks and global asset managers, in meeting privacy requirements and subsequent audits. As integrated compliance programs are instituted to comply with these regulatory demands, the institution must demonstrate its ongoing effectiveness in preventing the recurrence of privacy violations. This necessitates the development of a system capable of enforcing appropriate security measures, monitoring behaviour to ensure ongoing compliance, and auditing compliance at fixed intervals (Vil, 2010).

TECHNOLOGICAL SOLUTIONS FOR DATA PRIVACY

The European General Data Protection Regulation (GDPR) requires organisations to adhere to strict legal principles for data collection, processing, and storage, thereby enhancing user privacy. Unlike laws that leave compliance open to interpretation, GDPR explicitly mandates documentation of data control and processing activities (Georgiana Calancea et al., 2018). Since its principles are broad and technology-neutral, regulations require specific safeguarding and enforcement procedures when applied to particular technologies. Emerging contexts such as the Coronavirus Exposure Notification system and the Cloud Infrastructure Entitlement Management system (CIEM) illustrate where enforcement measures complement the interpretation and ethical use of existing regulatory principles. Web services have become the dominant model for Service-Oriented Architectures. Financial institutions (FIs) typically cash checks when customers provide proof of sufficient funds. Sometimes, FIS may link the reserved amounts to prevent multiple checks against the same balance. The FieldCrypt system ensures end-to-end security by encrypting XML fields in the client browser. It further secures its architecture by using proxy re-encryption to redirect XML fields at the SOA edge. In a FieldCrypt-enabled SOA network, an attacker who compromises an intermediate machine could swap, replay, or alter fields and documents passing through that machine. Web browsing transactions are also vulnerable to attacks from transaction generators, which wait for users to log in and then initiate transactions on their behalf (Spindel, Burnside, & Keromytis, 2009).

7.1. Privacy by Design Principles

Recent IT developments have driven technological evolution, enhancing economic productivity, knowledge work, and automation across industries. Respecting privacy as a human right has become crucial, leading clients to seek guaranteed confidentiality of their data. Designing IS involves creating an architecture that supports client goals before development, forming a logical framework capable of future functions. Traditional IS development begins with requirement analysis, viewing the IS as a system of integrated components. Assessing reliability is complex. Agile development emphasises requirements and preserves IS characteristics. Addressing privacy early in IS design, Privacy by Design (PbD) aims to embed privacy controls from the start. Though models illustrate privacy design implications, clear guidelines are lacking. Implementing PbD depends on integrating it into the IS lifecycle, which is common in organisations. PbD requires a mindset where privacy is guaranteed independently of practices, similar to IS security. Multiple strategies support PbD, including iterative privacy incorporation and general lifecycle guidelines. The most popular, by Ann Cavoukian, outlines seven principles—Proactive, Preventative, Default Privacy, Embedded Design, Full Functionality, End-to-End Security, Transparency, and User Privacy—that offer a comprehensive PbD framework. However, they lack a detailed application for IS development.

7.2. Role of Artificial Intelligence

The multifaceted concept of Artificial Intelligence (AI) and its numerous manifestations have garnered significant attention in the pursuit of pragmatic solutions for complex problems (Korobenko et al., 2024). Consequently, AI becomes an enabler of globalisation by providing an efficient mechanism to manage and process large volumes of data, such as the harmonisation and cross-referencing of global privacy frameworks.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Globally, the breakdown of national boundaries and the fluidity of human interaction have generated widespread repercussions for individual rights and liberties, thus requiring transparency in compliance with the regulatory system of the place where an individual resides—the dislocating intersection between local and national concerns (Lui & Lamb, 1970). As AI matures, it becomes instrumental in managing complex processes, similar to those experienced in the financial sector and retail banking, with applications ranging from voice recognition to chatbots, such as MScSgá[1]-le and Luvo, which assist customers through text or web chat (Humerick, 2018). Although concerns exist about the capabilities of and reliance on AI, financial regulators express confidence in aspects such as personalized customer services, the aggregation of fragmented data, control of risk, fraud detection, supervision of market conduct, investigation of market abuse, and the monitoring of financial stability—all of which highlight value propositions essential for the safety and soundness of the global financial system—and these same services are readily adaptable for the management of dynamic privacy frameworks. Nonetheless, the development of AI within cross-border financial institutions requires strict adherence to the synchronisation of regulatory principles and criteria aligned with the underlying rationale for protecting data privacy and maintaining institutional financial integrity (Adeyinka & Taiwo, 2024).

STAKEHOLDER PERSPECTIVES AND REGULATORS' VIEWS

Global financial institutions face challenges in aligning diverse international, sector-specific, and company-specific regulations within a broad privacy framework that supports cross-regional operations. Stakeholder perspectives are vital, with security, identity management, and data privacy as top concerns. A survey of 20 firms highlights controls, data audit, and identity management as impactful technologies in the next two years. Customer data privacy, identity, and payment security are key priorities, driven by third-party risk, breaches, regulations, and persistent attacks. Decision makers favour cross-sector frameworks over company-specific or sector-only approaches, emphasising the importance of maintaining operations despite regulatory differences. Regulators acknowledge the complexity, with laws applying differently across jurisdictions, and emphasise that compliance must align with both local and international laws, taking into account technical feasibility.

8.1. Financial Institutions' Perspectives on Consumer Attitudes toward Privacy

Financial regulators recognise that 'one-size-fits-all' privacy rules are not practical for global financial institutions. They suggest considering a consistent international approach to streamline implementation (A. de Dios, 2016). Secrecy laws in some countries protect bank privacy and client data from government and foreign access, but raise security concerns. Financial data repositories—containing tax, credit, transfer, and payment information—also spark privacy concerns, emphasising the need for safeguards. Prudential regulation is crucial, as larger, cross-border institutions face higher risks and sanctions. The Limited Global Public Interest Approach applies when products or services cross borders, necessitating the establishment of global standards, including those related to privacy and data protection. Organisations such as the OECD, Basel, IMF, G20, and FSB advocate for a comprehensive global financial framework that encompasses capital, risk, market discipline, and anti–money laundering measures. Frameworks outline principles, leaving details to national law, but a cross-jurisdictional view is vital for connected businesses (Mevorach, 2015). Consumers are largely unaware of privacy risks, though about 50% prefer to buy from privacy-focused companies (Srivastava, 2009). Privacy controls how much consumers can manage their personal information. Privacy invasion occurs when firms misuse personal data. US guidelines promote notice, choice, access, and security, with most research focusing on notice and consent. Less attention is given to benefits, risks, and fairness, while variables such as information type, demographics, and reputation influence privacy concerns and behaviour.

EMERGING GLOBAL STANDARDS AND FUTURE TRENDS IN DATA PRIVACY REGULATION

The global balance between privacy regulation and data-driven innovation remains elusive, but is intensifying (Hou, 2021). Disparate national regimes, vested interests, and the pace of change hinder cross-border cooperation. Recognising this, China's Cybersecurity Administration issued materials on China-EU privacy cooperation, detailed in the Cybersecurity Review Measures (CSRM) and the State Councillor's Economic Work Report. China's Law on the Protection of Consumer Rights serves as a guiding framework for the Data Security

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Law (DSL) and the Personal Information Protection Law (PIPL). Moving to enforceable standards will help regulators meet expectations. The PIPL's open architecture enables future norms, such as tracing and auditing, which facilitate compliance through technical measures. Similar principles to the EU's approach could limit data controllers' discretion and promote harmonisation, though the EU's complex rule-by-enum approach is not suitable for a global framework (F III Palmieri, 2019). A new model based on “behavioural efforts” respecting privacy rights is needed.

Public law should guide a global data privacy framework via treaties and agreements. China's admiration for the EU model suggests it will influence the new Global Privacy Framework (GPF). Harmonising GDPR, PIPL, and US orders is challenging but promising. As technology and financial markets evolve, cross-border institutions face increasing data and privacy risks. The OECD's 1980 privacy guidelines on data collection, quality, purpose, security, transparency, individual involvement, and accountability have influenced frameworks such as ISO, APEC, and GDPR. ISO's 2011 guidelines focus on privacy, transparency, and auditability in cloud services. The OECD updated its principles that year. The 2005 APEC Privacy Framework aims to protect privacy and ease data flow among 21 economies, emphasising security, limits, quality, notice, choice, accountability, monitoring, and access. The 2011 Cross-Border Privacy Rules foster trust by enforcing protections, ensuring agency accountability, and promoting compliance (Adeyinka & Kunle, 2024).

9.1 Impact of Technology on Future Regulations

Regulatory regimes require fundamentally new technology to process and act upon vast amounts of market data. Financial regulations can no longer be handled in the same manner as in the past. Big data and machine learning are now integral to economic regulation. Cross-disciplinary research among computer science, finance, sociology, management, and law is needed to examine the policy and legal consequences of technological decisions (L. Currie et al., 2018). Regulators also explore initiatives like regulatory sandboxes, which permit fintech innovation growth without imposing full regulatory obligations, aligning with principles-based regulation. The 2016 G20 Principles for Digital Financial Inclusion emphasise the establishment of flexible legal frameworks to enable fintech pilot projects. Traditional regulatory approaches are considered excessively burdensome, prompting new regtech startups, often backed by venture capital, to reduce complexity and lower entry barriers. The evolution of financial regulation depends on a sequenced approach to RegTech. Initially, a holistic strategy is essential for constructing contemporary market-supporting infrastructure, particularly in the global payments sector. Subsequently, appropriate regulatory responses to fintech innovation must be formulated through a multilevel framework with graduated requirements based on firms' risk profiles and sizes. Historical experiences in Africa and China illustrate the challenges associated with rapid development and the propensity for firms to attain systemic-importance status. System-wide monitoring is vital for regulators to comprehend emerging developments and their potential implications (Barberis, Ross P. Buckley, and Douglas W. Arner, 2017).

CONCLUSION

Across the globe, there is a convergence of priorities regarding data privacy and challenges associated with data flows across jurisdictions (Ramos & Solana, 2020). Financial institutions are establishing mechanisms to centralise data and customer information in regional hubs independent of organizational structure. These priorities and mechanisms align with global banking activity and the pursuit of common global privacy standards and mechanisms to facilitate responsible international data and information flows. The concluding section of the article, "Bank Resolution and Insolvency Law: The Tension Shaping Global Banking – Part II: The Cross-Border Dimension", synthesises previous parts, focusing on the conflicts that obstruct the consistency of global banking. The article notes that groups that are typically entangled in difficulties arise where activity has a genuinely multijurisdictional footprint. This ecological perspective on global banking structures brings a new dimension to the political economy of global banking, highlighting conflicts that revolve around the French and German approach, which favours simpler structures, versus the UK and US preference for structures that exploit tax and resolution arbitrage. The article surveys mechanisms for addressing cross-border banking conflicts, including conflict-of-laws analysis as applied to Europe’s extensive regulatory and judicial framework. The introduction of resolution procedures with the Bank Recovery and Resolution Directive (BRRD) is also examined,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

acknowledging advancement but also the emergence of new sources of conflict between regulators and supervisors in Europe. Efforts of the Financial Stability Board and the International Monetary Fund to steer global banking towards cooperation are described. The article concludes that the group is the appropriate frame of analysis and suggests improvements to address current obstacles to global consistency in banking structures.

REFERENCES

Ramos, D. & Solana, J. (2020). Bank resolution and insolvency law: the tension shaping global banking – Part II: the cross-border dimension. [PDF]

Kalogiannidis, S. (2024). Analysing the Challenges of Cross-Border Disaster Response and Management: A European Perspective. Journal of Risk Analysis and Crisis Response. jracr.com

Fiero, A. W. & Beier, E. (2022). New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation. Stan. J. Int'l L.. [HTML]

Babikian, J. (2023). Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. Law Research Journal. lawresearchreview.com

Maria Lopes, I. & Oliveira, P. (2018). Implementation of the general data protection regulation: a survey in health clinics. [PDF]

Sirur, S., R. C. Nurse, J., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). [PDF]

Birrell, E., Rodolitz, J., Ding, A., Lee, J., McReynolds, E., Hutson, J., & Lerner, A. (2023). SoK: Technical Implementation and Human Impact of Internet Privacy Regulations. [PDF]

Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C., & Egelman, S. (2023). Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA). [PDF]

Akindele, R. (2017). Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system. [PDF]

D. Mitchell, A., & Hepburn, J. (2018). DONu27T FENCE ME IN: REFORMING TRADE AND INVESTMENT LAW TO FACILITATE CROSS-BORDER DATA TRANSFER BETTER. [PDF]

Pearce, G. & Platten, N. (1998). Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective. [PDF]

Corley, M. (2016). The Need for an International Convention on Data Privacy: Taking a Cue from the CISG. [PDF]

Marelli, M. (2024). Transferring personal data to international organisations under the GDPR: an analysis of the transfer mechanisms. International Data Privacy Law. oup.com

Vil, J. (2010). Integrated Compliance Framework for Data Processing Applications. [PDF]

Kulesza, J. (2012). Walled Gardens of Privacy or "Binding Corporate Rules?"A Critical Look at International Protection of Online Privacy. [PDF]

Adeyinka, O. & Taiwo, A. (2024). Enhancing Waste Management Efficiency through Strategic Logistics Optimization. International Journal of Sustainable Engineering and Environmental Technologies, 5(2), 1-9. https://doi.org/10.5281/zenodo.14535876

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2022). Exploring the Relationships between Privacy by Design Schemes and Privacy Laws: A Comparative Analysis. [PDF]

Xi, W. (2024). Regulatory Changes and Compliance Challenges. In Strategic Financial Management: A Managerial Approach (pp. 119–134). Emerald Publishing Limited. [HTML]

Elliott, K., Coopamootoo, K., Curran, E., Ezhilchelvan, P., Finnigan, S., Horsfall, D., Ma, Z., Ng, M., Spiliotopoulos, T., Wu, H., & van Moorsel, A. (2021). Know Your Customer: Balancing Innovation and Regulation for Financial Inclusion. [PDF]

Coley, A. (2017). International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà Vu. [PDF]

A de Dios, M. (2016). The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy. [PDF]

Georgiana Calancea, C., Alboaie, L., & Panu, A. (2018). A SwarmESB-Based Architecture for a European Healthcare Insurance System in Compliance with GDPR. [PDF]

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VIII August 2025

Spindel Burnside, M., & D. Keromytis, A. (2009). FieldCrypt: End-to-End Protection of Sensitive Information in Web Services. [PDF]
Foujdar, A. (2019). Implementing Privacy by Design through Privacy Impact Assessments. [PDF]
Skinner, G. & Chang, E. (2005). PP-SDLC: The privacy-protecting systems development life cycle. [PDF]
Korobenko, D., Nikiforova, A., & Sharma, R. (2024). Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems. [PDF]
Lui, A. & Lamb, G. (1970). Artificial intelligence and augmented intelligence collaboration: Regaining trust and confidence in the financial sector. [PDF]
Oluwayemisi Adeyinka, & Kunle Akanbi. (2024). The Impact of Transportation Intervention on Public Health Care Outcome. International Journal of Innovative Science and Research Technology (IJISRT), 9(12), 617–623.
Humerick, M. (2018). Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence. [PDF]
Hou, B. (2021). A Novel Data Governance Scheme Based on Behavioural Economics Theory. osf.io
Mevorach, I. (2015). Beyond the search for certainty: addressing the cross-border resolution gap. [PDF]
Srivastava, M. (2009). Consumers' Cognitive, Affective, and Behavioural Responses to an Invasion of Privacy: Essays on Understanding Consumers' Privacy Concerns. [PDF]
F III Palmieri, N. (2019). Data Protection in an Increasingly Globalised World. [PDF]
L. Currie, W., P. Gozman, D., & J. M. Seddon, J. (2018). Dialectic tensions in the financial markets: a longitudinal study of pre- and post-crisis regulatory technology. [PDF]
Barberis & Ross P. Buckley Douglas W. Arner, J. (2017). FinTech, RegTech, and the Reconceptualisation of Financial Regulation. [PDF]