ISSN (Print): 2959-4391 ISSN (Online): 2959-4405

JOURNAL OF SOCIAL SCIENCES DEVELOPMENT

www.jssd.org.pk editor@jssd.org.pk

BRIDGING THE GAP: CROSS-BORDER DATA FLOWS & DATA PROTECTION HARMONIZATION IN PAKISTAN

Lubaisha Bint Sohrab[1], Kainaat Shah[2] & Bushra Nawaz[3]

[1]Lecturer Department of Law, Mohi-Ud-Din Islamic University Nerian Sharif, AJ&K, Pakistan
[2]Advocate High Court, Khyber Pakhtunkhwa Bar Association, KP, Pakistan
[3]Lecturer, Department of Law, Mirpur University of Science & Technology, Mirpur, Pakistan

KEYWORDS

Data Flows, Data Privacy, GDPR Compliance, CBPR Adoption, Data Sovereignty, Digital Trade.

ARTICLE HISTORY

Date of Submission: 27-08-2024
Date of Acceptance: 29-09-2024
Date of Publication: 30-09-2024

ABSTRACT

The data protection complexities between Pakistan and other nations are investigated in this study. Given that Pakistan's technological marketplace is rapidly increasing, it becomes imperative for Pakistanis to understand the subtleties of data protection laws across jurisdictional borders. A thorough analysis is made of Pakistani legislation structures, focusing on the proposal of Data Protection Legislation and its relevance to international regulations namely European Union Regulations & Asia Pacific Economic Cooperation. The legislative deficiencies identified are significant & relate to protocols of transnational information exchange, safeguards in place for individuals, & measures of regulatory execution. These regulatory gaps create commercial ambiguities & prevent international data exchange operations. There is a need for establishment of information protection legislation & clarification of trans-border exchange is echoed in administrative suggestions. Pakistan could set up invincible informational security steps, which fortify business confidence, fortify fiscal development, and guard individual privileges in the current technological foundation, over systematic settlement of these administrative obstacles.

Corresponding Author Lubaisha Bint Sohrab

Email: lubaisha.21@gmail.com

DOI https://doi.org/10.53664/JSSD/03-03-2024-19-232-247

INTRODUCTION

The twenty-first century globalized economy has been characterized by a rapid and seamless flow of information, capital and goods across borders, due to progress in the digital technologies. The interconnectedness has changed the way that business operates, giving them the ability to transact across borders with the ease never seen before. The cross-border flow of data is one of the critical issues of this landscape; thus, data are seen as one of the prerequisites for several business processes,

such as communication, marketing, financial transactions and data analysis. The ability of data flows to increase productivity and promote growth in national economies through evidence that digital trade increases growth in gross domestic product (GDP) more than traditional goods trade does (Wang, 2023; Cory, 2022) highlights their importance. In the case of Pakistan, this growing digital economy has led to reliance on cross-border data flows. By Wang (2023) and Wang (2021), owing to significant growth in the internet penetration and mobile phone usage in the country, e-commerce has expanded because e-commerce and Pakistani businesses have been able to enter international markets.

However, they also create challenges with data flows, including data sovereignty and regulatory compliance. As data move across national borders, they enter the jurisdiction of many laws at once (Casalini et al., 2021; Mitchell & Mishra, 2019), which is a complex legal landscape that businesses are fitted to traverse. Moreover, the approaches to data sovereignty taken by various countries are remarkably diverse, ranging from strict requirements of data localization to slightly more flexible programs, permitting cross-border transfers under certain conditions (Ferracane et al., 2019). It is particularly relevant to Pakistani business, as most of our business is still under data protection legislation for safe data transfers to build trust among global partners. The Personal Data Protection Bill represents an enormous step in the direction of setting up a robust legal structure, although its complete enactment, along with alignment with international standards such as European Union's General Data Protection Regulation is pending (Yakovleva, 2020). The country gap amid domestic laws and international standards poses a compliance issue, businesses must comply with more rigid conditions when managing the international data, even if such laws are not enforced in Pakistan (Guamán et al, 2021).

The end result of this situation can create greater compliance costs and increased legal complexity, hindering the ability of Pakistani businesses to compete in the global digital economy (Challapalli, 2023). This research seeks to examine these frameworks from the perspective of international data protection standards and examine whether these frameworks address these challenges. Research can serve to identify key gaps and inconsistencies and recommend policies to strengthen the data protection regulations and regulators' harmonization (Thaldar, 2023). For Pakistan, leveraging the cross-border data flows presents significant opportunities to enhance its digital economy, attract foreign investment, and integrate into the global value chains. In addition, we examine practical strategies for compliance and demonstrate how these strategies can help Pakistani businesses navigate the complex terrain of the cross-border data flows to facilitate international trade and collaboration to foster economic growth while ensuring data security and privacy (Wang, 2021). Finally, this research aims to help develop a better and harmonized data protection framework in Pakistani context, bolster trust and enable businesses to manage their trade in the ever-evolving, digital economy.

LITERATURE REVIEW

In the globalized digital economy, where cross-border data flows are increasingly driving trade, robust legal frameworks are needed to balance the ease of trade with the protection of data privacy (Wang, 2023; Cory, 2022). Although digital trade obviously leads to greater GDP growth (Wang,

2023; Wang, 2021), achieving international data governance associated with digital trade is a daunting task (Mitchell & Mishra, 2019). In addition, the complexity of compliance in this space is further compounded by diversity of methods used to attain data sovereignty from strict localization to conditional transfers (Ferracane et al., 2019). In a broader sense, it is particularly pertinent to Pakistan, which is still at infancy of developing its legal landscape. The Personal Data Protection Bill entails progress, but its enactment and alignment with international standards, such as GDPR, has yet to be made (Yakovleva, 2020). Still, this discrepancy generates compliance challenges that can result in higher costs and impede competitiveness (Guamán et al., 2021; Challapalli, 2023). According to Thaldar (2023); Wang (2021), data protection regulation & regulatory harmonization should be promoted.

More broadly, this entails filling in the gaps in draft legislation such as Pakistan's Prevention of Electronic Crimes Act (PECA), which nonetheless fails to spell out how to manage cross-border data transfers (Dhirani, 2024; Salsabila & Ilmih, 2024). Moreover, PECA's data retention requirements and expansive investigative powers cause privacy concerns and noncompliance with international standards (Dhirani, 2024; Khanna, 2024). While sector-specific regulations are laid down, cross-border transfers are not clear (Dhirani 2024, Shrestha 2020). Thus, the picture is also made further murky by the global push for data sovereignty and localization, which impacts both international business and local legal frameworks (Jansen et al., 2023; Singi et al., 2020; Ismagilova & Карине, 2020; Coche et al., 2023). This demonstrates the necessity of strict rules, methods, and international collaboration to pass on the chaos of cross-border data streams and retain data security principles (Coche et al., 2023; Raab, 2010). Although it does not mention the data protection directly, the constitutional right to privacy provides the scaffolding for this to be built on in Pakistan in a manner that is in line with the waves around the world that promote privacy as a fundamental right (Nair, 2024; Madiev, 2023; Luna and Maxhelaku, 2023; Singh, 2024; Primec et al., 2024; Gulyamov and Raimberdiyev, 2023).

RESEARCH METHODOLOGY

A qualitative methodology has been applied in this research, which draws upon an extensive review and study of the literature on cross-border data flows, regulatory harmonization and data protection frameworks. The study's sources are academic articles, legal texts, policy documents, industry reports and expert commentary. A systematic literature search was performed over a set of keywords, including cross border data flows, data protection, regulatory harmonization, Pakistan, "GDPR", "APEC". Scholarly articles and legal materials were sought from institutional and reputable databases, such as JSTOR, ScienceDirect, LexisNexis and HeinOnline. The selection criteria were prioritized on basis of official documents and peer-reviewed publications cited by governmental and international organizations towards the growing reliance upon international digital platforms and services. In this regard, thematic analysis was performed on collected literature to realize the key trends, challenges and opportunities in cross-border data flows in Pakistan. This qualitative approach is advantageous in that it allows in-depth examination of maze of legal and regulatory settings and the ins and outs of problems faced by Pakistani businesses operating in the globalized digital economy.

RESULTS OF STUDY

This qualitative study reveals a wide gap between what the existing legal frameworks of Pakistan on cross-border data flows allow for and the international standards in place. It argues that there are ambiguities and infelicities about such mechanisms of data transfer, individual rights of data subjects and enforcement ability concerning Pakistani laws such as draft Pakistan Personal Data Protection Bill and the Prevention of Electronic Crimes Act. In contrast to international frameworks like GDPR and APEC CBPR, Pakistan's legal landscape needs a more comprehensive composition to provide appropriate and necessary data protection when data are across borders. The study revealed areas of confusion around adequacy choices, weakly developed data subject rights, and weak enforcement machines that can keep Pakistani companies from tackling international issues. In addition, data localization requirements have reignited debates, with businesses needing to decide whether they should leverage their global IT infrastructure. This result highlights the need to strengthen Pakistan's data protection framework, as it aligns with international best practices, shows compliance, and provides confidence in cross-border data transactions. The study identified practical ways businesses can negotiate this cumbersome regulatory space while protecting data and facilitating trade.

Legal Frameworks in Pakistan and International Alignment

Analysis of Pakistan's Legal Landscape

Currently, Pakistan's data protection landscape is fragmented, comprising various piecemeal laws and the yet-to-be-enacted Personal Data Protection Bill 2020 (PDPB), which aims to establish a cohesive data protection framework. According to PDPB, key international best practice principles (data localization requirements, adequacy decisions, consent for cross-border data transfers) have been incorporated into its provisions. The previous versions of the bill demanded strict localization of data. However, the most recent ones adopt a more flexible approach to understanding digital economy international data flows (Coche et al., 2023; Ismagilova & Карине, 2020). Adequacy decisions that determine the level of data protection in countries receiving data from Europe are nebulous in bill and are uncertain for businesses in international data transfers (Coche et al., 2023). There is a focus on consent and contractual clauses for cross-border data transfers that match global trends, but requirements of these clauses are not detailed (Coche et al., 2023). Second, exemptions for national security and law enforcement purposes under PDPB need more clarification to avoid their misuse while preventing the conflation of data protection and other fully legitimate interests (Coche et al., 2023).

At the regional and international levels, regional and international frameworks, including the EU's GDPR, establish parameters for designing national laws tailored for Pakistan (Hayat, 2007; Singi et al., 2020). However, the problems faced by Pakistan are not peculiar; these problems are common to many countries trying to reconcile the protection of data and free flow of information while being the part of regional trade agreements that either allow or restrict data flows (Słok & Mazur, 2023; Mattoo & Meltzer, 2018). Also, both globally and in Pakistan, the push towards digital sovereignty and data localization stems from need for privacy and security within the evolving legal framework (Jansen et al., 2023; Singi et al., 2020). This is part of trend whereby more countries are beginning

to realize importance of having a robust data protection law that allows international businesses to protect their privacy and essential for trust-building with international partners and attracting investment. (Ismagilova & Карине, 2020; Coche et al., 2023). As Pakistan has improved its data protection laws, it needs to wade through these complex regulatory spaces to achieve compliance & establish international cooperation (Raab, 2010). In addition to cybercrime, PECA also takes care of data protection.

The relevant provisions include the following: In Pakistan, the other cybercrime is the Prevention of Electronic Crimes Act, 2016 (PECA), which concerns itself with cybercrime but includes general aspects of data protection, such as unauthorized access, data breaches, data retention, and powers of investigation and surveillance. Because it is overly broad, PECA makes it a crime to gain the unauthorized access to data & data breaches without offering clear directives for the cross-border data transfer and lawful processing of data (Dhirani, 2024). Considering the global nature of cyber threats and cooperation on data protection, which are hallmarks of the General Data Protection Regulation (GDPR) in the European Union as guideline for stiff data protection laws (Salsabila & Ilmih, 2024), this gap is massive. Moreover, PECA data retention requirements for service providers could contradict international data protection laws by necessitating the multilayered compliance issue for cross-border data flows (Dhirani, 2024). Accordingly, act also provides law enforcement agencies with broad powers to acquire and intercept data, which could be infringement of privacy and will require fine harmony among the security requirements and the long right of the individual (Khanna, 2024).

Data protection in Pakistan is also regulated by sector-specific regulations on banking, telecom, power, and healthcare. Financial institutions in Pakistan must follow data security measures as per the State Bank of Pakistan and international best practices (PCI DSS) as per the mandate (Dhirani, 2024); however, all these measures are for financial sector and hence may be incomplete for other sectors for data protection principles (Shrestha, 2020). In telecom, data privacy is regulated by the Pakistan Telecommunication Authority, but data transfers beyond its borders are not clear (Dhirani, 2024). Emerging regulations in the health care sector include patient data privacy, while a framework for the protection and cross-border transfer of data is still in its initial stages (Dhirani, 2024). This interplay highlights need for more harmonized data protection regulations in Pakistan as response to globalized data governance-driven data protection norms and individual data rights in context of a global digital society (Zubaedah et al., 2024). The fragmented nature of Pakistan's legal landscape creates several ambiguities and potential conflicts. In Pakistan, legal land space of data protection and cybersecurity is very fragmented, gives rise to many ambiguities and conflicts in the legal space.

The knowledge in data collection and processing methods also grows rapidly as a consequence of digital technologies like AI and IoT development, causing amendments in regulation frameworks to protect the privacy of individuals while embracing innovation (Singh, 2024; Primec et al., 2024). The privacy and information security are among the key areas of review since data vulnerabilities democratize information and accumulate systemic corruption and abuse, the awareness of which requires strengthening data protection activities (Gulyamov & Raimberdiyev, 2023). Moreover,

digital constitutionalism stresses the application of traditional constitutional values to the virtual realm and the demand for a guarantee of human rights and 'rule of law' in the information society (Walter, 2022). In this context, Pakistan's legal scene should duly respond to debatable concepts, convergence, and probable clashes between current relevant laws and enactments to construct a comprehensive and coherent data protection regime that matches the international standards and promotes Pakistan's thriving digital economy (Pang, 2022). In this connection, this analysis serves as a basis for assessing Pakistan's framework, with international standards directing the gaps and inconsistencies to be filled to qualify for comprehensive data protection and privacy rights in the digital era.

Comparison with International Standards

This part of the research compares Pakistan's legal framework (particularly the draft Personal Data Protection Bill (PDPB) with key international data protection standards in terms of key principles only. A comparison will showcase areas of convergence and divergence to narrate where Pakistan stands in alignment with and divergence from the global best practices toward the harmonization of the data protection regime. General Data Protection Regulation (GDPR – EU): Among other data protection regimes, the General Data Protection Regulation (GDPR) of European Union is a wide-ranging framework that dictates the data minimization, purpose limitations, data subject rights, accountability, and cross-border data transfers to an elevated standard globally. It provides robust data subject rights beyond those in PDPB for access, rectification, erasure, data portability and the right to object to automated processes (Ref1). Data minimization under the GDPR is founded on the privacy-by-design principle that an organization collects only data needed for specified purposes (Ganesh et al., 2024) to lessen the risk of data breach and unauthorized access. Data minimization was specified more granularly than other committees such as the PDPB (Singh, 2024), and the GDPR provides detailed guidance for implementation, such as defining data types and the data retention period.

Additionally, purpose limitations are another essential element: the GDPR sets strong requirements for collecting consent for secondary data usage so that data are used only for the initial objective (Padrão et al., 2023). This follows requirements of performing mandatory data protection impact assessments and appointing data protection officers so that organizations demonstrate compliance with data protection principles (Singh, 2024; Bertolaccini et al., 2023). The GDPR requires that organizations securely transfer the cross-border data, ensuring adequate protection when recipient countries, allowing for adequacy decisions and standard contract clauses (Akhtamovna, 2023). In this linking, its stringent requirements and the requirement of hefty penalties for noncompliance, including a fine of up to 4% of a company's global annual turnover, have led the GDPR to shape data protection practices and influence global data governance and management (Bakare et al., 2024). Still, it has imprecise and missing enforcement mechanisms compared with prescriptive frameworks such as the GDPR and CBPR. Despite the fact that the regulation affects international businesses that manage the data of EU citizens, compliance is necessary for international businesses that deal with the data of EU citizens and thus requires an initiative-taking approach (Bertolaccini et al., 2023).

By infusing transparency, accountability and individual rights into the regulation of personal data protection, GDPR has changed the dynamics of personal data protection by establishing a baseline for protecting personal data under proposed data privacy law at the global level (Nasiadka, 2023). APEC cross-border privacy rules: The APEC cross-border privacy rules system is a strong framework that provides recognition by the participating economies of each other's data protection standards and facilitates cross-border data transfers between economies participating in system. The eight privacy principles they based on are preventing harm, noticing, collection limitations, use diverse limitations, the data quality, security safeguards, access and correction, and accountability, which completely match Personal Data Protection Bill principles except for more detailed guidance on how to implement principles and have a certification method to demonstrate compliance. A CBPR system, which mandates that organizations name as accountability agents] those who will ensure that they are navigating the system appropriately and handling complaints, is vital CBPR requisite that the PDPB fails to address properly, possibly diminishing the latter's accountability framework (Sarabdeen, 2024).

While the PDPB's framework for cross-border transfers is still not well developed, the CBPR offers a streamlined approach of certified organizations that offer an adequate level of protection, which facilitates smooth international data flows (Singh & Prerna, 2024). Particularly, relevant to the global trade and digital economy, where data have become the key factor of the productivity and international cooperation (Zhang, 2024), CBPR's approach to cross-border data transfers resembles the proposals the ODIHR put forward in the study of cross-border data flows. While the APEC framework has been criticized for establishing a lower standard than the EU's GDPR, setting APEC and EU frameworks of privacy in opposite areas threatens to create privacy confrontations between regions (Greenleaf, 2004). However, these criticisms notwithstanding, the CBPR system represents a large step toward a coordinated approach to privacy standards in the Asia-Pacific region, which in turn leads to both economic benefits from the trade of personal data and its protection (Greenleaf, 2006; Greenleaf, 2004). This emphasis on accountability and certification would provide a model for other regions' balance between privacy safeguarding and facilitating cross-border data flows (Malahleka, 2024).

In principle, the PDPB aligns itself with these frameworks but does not reflect the level of provisions or the enforcement that the GDPR has been impetus behind (Maurya & Prasad, 2021). In ongoing work by the OECD, including the Recommendation on Health Data Governance, data frameworks are necessary to balance benefits of data-driven innovation with data protection (OECD, 2022). In addition, studies reviewing global landscape of data privacy laws emphasize technical challenges and the demand for competencies in addressing technological advances such as cross-border data flows and digital surveillance (Ehimuan et al., 2024; Chen, 2021). The PDPB's present limitations in those areas indicate that a change is needed to be in line with global benchmarks and to effectively manage the intricacies of contemporary data governance (Maurya & Prasad, 2021). The GDPR and CBPR, not only for their detailed requirements but also for their robust enforcement frameworks, represent good benchmarks for improving PDPB so that Pakistan data protection regime matches international standards of adequate protection. These results are then used in the next section to

conduct the gap analysis, leading to a meaningful discussion of the particular areas of Pakistan's framework that need to be settled further to reach international benchmarks for dealing with cross-border data flows.

Gap Analysis & Inconsistencies

This section examines where specific gaps and inconsistencies between Pakistan's legal framework for data protection and cross-border data transfers and established international standards reside. This analysis helps Pakistani businesses operating in the new digital economy understand the key challenges they face. An analysis of Pakistan's existing legal framework for data protection and cross-border data transfers reveals several gaps and inconsistencies vis-à-vis the well-established international standards set by the European Union's General Data Protection Regulation (GDPR). The most important gap, however, is lack of a fully enacted, comprehensive law on data protection, in which the Personal Data Protection Bill (PDPB) 2020 remains unenacted, in contrast with robust frameworks such as the GDPR for businesses (Dhirani, 2024; Kwon et al., 2023). In this connection, the absence of comprehensive legislation makes compliance processes difficult for the Pakistani businesses, thereby putting them at the disadvantage in global trade (Ferracane & Marel, 2024). Additionally, the PDPB lacks clarifications on cross-border data transfer mechanisms compared with those of GDPR, complicating cross-border data transfer for businesses (Singh & Prerna, 2024; Ashutosh, 2024).

In addition, these challenges are aggravated by the limited scope of data subject rights under the PDPB, e.g., the lack of explicit data portability rights, which results in conflicts when operating in cooperation with other jurisdictions where data protection rights are stronger (Kwon et al., 2023). In addition, Pakistan's regulatory framework creates other challenges in achieving effective data protection through weak enforcement mechanisms, which lack significant penalty & independent supervisory authority that would come with the GDPR (Dhirani, 2024). With businesses potentially unable to utilize global IT infrastructure, strict localization requirements within PDPB contribute to uncertainty (Lyu, 2024; Singh & Prerna, 2024). In addition, the PDPB does not provide the clear instructions on the processing of the sensitive personal data (including health and biometric data), which fall into a stricter category established by internationally recognized standards (Duravkin & Hafych, 2023). In this linking, these gaps and inconsistencies are indicative of the sufficient legislative development that Pakistan needs to undergo to harmonize its data protection laws with the international norms and standards for the sake of businesses' global operations and the privacy rights of individuals.

Table 1 Quantifying the Gaps: A Comparative Table

Feature	GDPR	PDPB (2020 Draft)
Comprehensive Law	Yes	Pending Enactment
Adequacy Decisions	Detailed Criteria & Process	Ambiguous Criteria
Contractual Clauses	Specific Requirements Defined	Limited Guidance
Data Portability Right	Yes	Not Explicitly Addressed
Data Subject Rights	Strong, Independent Authority	Enforcement Mechanisms
Enforcement		Under Development

Data Breach Notification	Mandatory & Time-Bound	Provisions Included but Details Need Clarity
Financial Penalties	Significant & Dissuasive	Penalty Structure Needs Further Definition

This table clearly shows that the principal areas that need to be improved in Pakistan's framework are consistent with international standards. We cannot establish a precise scoring system because of the fluidity of the PDPB, but the table qualitatively illustrates how wide the gaps are. Such gaps and inconsistencies create significant trouble for Pakistani businesses aiming to participate in cross-border data flow within rule book of domestic & international regulations. These challenges are critical to address to build trust, facilitate international trade and grow the digital economy of Pakistan. In the following chapter, we discuss practical strategies for businesses to do so within this regulatory mire.

Practical Strategies for Businesses: Achieving Compliance & Fostering Collaboration

There are many issues for Pakistani businesses to consider when control international data transfers, namely, how to maintain minimal awareness of and adaptability to the international standards of data protection, together with GDPR. A) This is compounded by absence of domestic comprehensive data protection law and (weak) enforcement of existing regulations, leading to a general lag in the adoption of these standards, mainly by SMEs (Javed et al., 2020; Coche et al., 2023). The ability to obtain consent from data subjects for transfer of data across borders is legally valid but not almost or effectively feasible for mass data transfers (Gunasekara, 2006; Power & Trope, 2005). Moreover, there is a shortage of clear guidance under Pakistani law with respect to use of standard contractual clauses and other transfer mechanisms (Słok & Mazur, 2023). Even more complex is the debate over data localization, which causes uncertainty in cross-border data flows, as local policies continue to be volatile (Fratini & Musiani, 2024). Without standard national data protection laws, Pakistani businesses are not compliant with international regulations, creating a roadblock in their trade and collaboration with the world (Cheema et al., 2023). These challenges indicate the need for better regulatory frameworks, increased knowledge & increased implementation of Pakistan international data protection standards to enable more secure and more efficient border data transfer (Proudfoot et al., 2024).

Current Practices of Pakistani Businesses

Coming on board with both global data protection and data transfer standards in the international market will help Pakistani businesses increase their reputation and be able to sell abroad and trade internationally without a hitch. Therefore, this initiative-taking approach is vital, especially given the fragile nature of international partners, to help build trust and increase easier cross-border operations even in the absence of strict local regulations (Mattou & Meltzer, 2018; Ismagilova & Карине, 2020). As mentioned previously, a second effective method to safeguard your data is to implement robust data security infrastructure and teach your people about data protection to the fullest. Using this investment, companies can prepare themselves to manage the cross-border data flows safely and meet global regulations, such as the GDPR, which has adopted an international standard for data protection (Kuner et al., 2017). This thorny data protection and transfer world of

cross-border data transfers necessitates some engagement with diverse legal and technical experts. However, implementing effective compliance solutions in companies depends on engagement with businesses because listed countries are not uniform with their regulatory approach, from the quite stringent, such as the data localization requirements, to liberal (Kuner et al., 2017; Ismagilova & Карине, 2020).

Best practice transfer depends on trust and reputation; the greater degree of trust and reputation, the greater the degree to which employees are willing to observe best practices and adopt new practices (Lucas, 2005). Moreover, the phenomenon of internal transfer of best practices associated with people as the organizations' greatest assets and organizational knowledge, which is part of the outdated knowledge embedded within organizations, involves knowledge that can be transferred horizontally amid organizations, which involves employee involvement and open communication (Zairi, 2000) and can be modeled on cross-border knowledge transfer. In addition, the integration of a blockchain-type decentralized mechanism for cross-border identity authentication shows that innovative approaches can be used by businesses to improve data security and privacy for their international operations (Chen et al., 2024). In this connection, the strong data protection laws increase consumer confidence in digital platforms, fostering local and international e-commerce. Overall, various strategies have been presented. These strategies should be more aware of capacity building and provide practical guidance for businesses in Pakistan to improve compliance and international participation while addressing the challenges of the (Chan et al., 2024) cross-border data flows.

Best Practices for Compliance

Pakistani businesses performing cross-border data transfers can adopt several best practices to adhere to domestic and international jurisdictions for data protection. Data protection by design and default needs to be implemented, which means a need to design products and services so that data protection principles may be built into them to minimize data collection and be transparent to data subjects (Chhetri et al., 2022; Lohmann, 2011). Thus, another important strategy is data transfer impact assessment, allows businesses to analyze 'risks' and identify 'safeguards' before transferring personal data across borders (Li et al., 2021). According to the regulations of the GDPR (Guamán et al., 2021), data transfers present approved mechanisms, including BCRs. On another note, evolving comprehensive data protection policies that are regularly updated and available to data subjects will increase compliance (Hamou & Hamou, 2007). Data protection principles need to be trained for employees, as encourage a data protection culture and reduce data breaches (Li et al., 2021). Although such an appointment is not mandatory under Pakistani law, businesses using significant volumes of personal data may wish to appoint data protection officer for compliance, engagement with data protection authorities (Mattoo & Meltzer, 2018). These strategies allow the businesses to manage cross-border contexts, complying with relevant data protection regulations & protecting personal data.

Fostering International Trade and Collaboration

The international trade and collaboration are increasingly recognized as strategic opportunities for enhancing compliance with data protection regulations, not just as a legal necessity. Trust helps

build reputation, and those companies that show a strong commitment to data security will have a competitive advantage by having trust of customers, partners and investors. In today's globalized economy, where data are valuable assets (Irion & Yakovleva, 2020; Irion & Yakovleva, 2019), this is especially important. Another major benefit is cross-border data flows; robust data protection measures can help to facilitate cross-border data flows by reducing the transaction costs and legal uncertainties, thus enabling business transactions across borders to be performed smoothly (Kong, 2010) (Gao et al., 2023). In sectors such as e-commerce and financial services, data privacy and security are of paramount importance, and leveraging data protection as a competitive advantage becomes particularly important, attracting customers who are increasingly worried about how their data are being utilized (Kuner et al., 2017; Słok & Mazur, 2023). Applying these best practices helps businesses (also in Pakistan) seamlessly manage the cross-border data transfer issues, improve compliance efforts, and participate in the growth of the digital economy (Coche et al., 2023; Słok & Mazur, 2023).

DISCUSSION

This looks illuminating where Pakistan's data protection framework has been. The analysis shows that the Personal Data Protection Bill appears to be right step toward conforming to international standards. However, there are serious gaps that need to be addressed urgently. A lack of a fully enacted comprehensive law yields uncertainty for businesses in terms of being able to engage in cross-border data flowing confidently. Ambiguities around mechanisms for the cross-border data transfer, rudimentary enforcement and the poor data subject rights compound these. The Pakistani businesses operate in complex and often contradictory compliance environments that may impede their international competitiveness. In this connection, the PDPB is compared against international standards, namely, the GDPR and CBPR frameworks of APECs and deficiencies in the PDPB are identified. To align with global best practices, Pakistan's data protection regime needs the clearer criteria for the adequacy decisions and robust data subject rights with the stronger enforcement mechanisms. If we can close these gaps, that will help us with compliance. However, it will also help us to build the desired trust and enable trade, international trade, and international collaboration win for everybody.

In addition, the careful thought must be given to the current confusion on the data localization requirements of businesses in a globalized digital economy that want the same data sovereignty they have but practical needs. The fact that act of enacting PDPB is delayed complicates situation even further. It delays uncertainty and hinders the growth of a stable and predictable regulatory environment. Currently, Pakistan is finalizing and implementing a broad-based data protection law in accordance with international standards. This problem requires precision detailed provisions on cross-border data transfer, robust data subject rights & effective enforcement mechanisms. Just as important is constructing dialogs and conferences between the government and the think-and-do tank. The public should ensure a data protection framework consensus that aligns all interests and is useful for making a vibrant digital economy. This is an even greater reason to intensify efforts to close gaps identified & adoption of data protection regime in Pakistan that will increase domestic

business volume while meeting requirements to stay within bounds that protect individual privacy in digital age.

CONCLUSION

This research examines the critical issues of cross-border data flows and regulatory harmonization in Pakistan. A nascent but developing data protection landscape was analyzed, which included the development of comprehensive data protection law. Although well-intentioned, the Personal Data Protection Bill has long way to go regarding its cross-border data transfer mechanism, data subject rights and enforcement capabilities. Still, these gaps have made it difficult for Pakistani business, which, along with a multinational company wanting to hire in Pakistan and adhering to local and international online privacy laws, presents a considerable challenge in addressing these gaps. The need to adapt Pakistan's framework is similar to international best practices in building trust and supporting international trade. Pakistan is still aiming for economic expansion and insertion in the global digital economy, so Pakistan's cross-border data flow must also be effectively governed. For businesses to comply and for every individual to have control over personal data, the gaps and inconsistencies in legal framework need to be addressed. A key next step should be enacting strong data protection law, establishing mechanism for cross-border transfer and improving enforcement. However, we have to engage government, private sector, civil society to help build data protection regime in Pakistan that squarely reflects interests of all stakeholders while ensuring growth of a digital ecosystem. This research is clarion call for governments & businesses to take data protection on board as strategic imperative & to come together to create environment of trustworthy data flows in digital era.

Business Recommendations

1. Conducting data transfer impact assessments: Check the risks of cross-border data transfers and take appropriate safeguards.
2. Adopt Standard Contractual Clauses: Transferring data to countries without adequacy decisions to countries with standard contractual clauses or other appropriate means.
3. Implement Data Security Measures: Invest in robust data security measures to protect sensitive data from unauthorized access and breaches.
4. Enhance Transparency: You should ensure that data subjects are aware of clear and easy-to-understand privacy policies for cross-border data transfers.
5. Stay Informed: Be aware of the new data protection laws current in Pakistan as well as at the national level.

Policy Recommendations

1. Enacting the PDPB: This reinforces the need for the Personal Data Protection Bill, along with clear rules for cross-border data transfers, robust data subject rights, and strong enforcement mechanisms.
2. Clarify adequacy decisions: This work aims to clarify the standards for assessing adequacy of the level of data protection in recipient countries.
3. Strengthen Enforcement: Meets resource and capacity building needs in facilitating the enforcement of data protection laws.

4. Promote Harmonization: Participating actively in the international forums, lobbying for the harmonization of data protection rules and permitting cross-border data flows.

REFERENCES

Aaditya, M., & Joshua, P. (2018). International data flows and privacy: the conflict and its resolution. *Journal of International Economic Law*, DOI: 10.1093/JIEL/JGY044.

Aftab, A. (2024). The Dilemma of Free Speech: Confrontations and Restrictions in Pakistan. *Journal of social sciences review*, DOI: 10.54183/JSSR.V4I1.399.

Aizaz, K., Zohaib, H., Shozeb, H., & Khalequ, Z. (2023). A critical examination of the entanglement: How political dynamics shape legal Decision-making and reform processes in Pakistan. *International Journal of Multidisciplinary Research & Growth Evaluation*, DOI: 10.54660/.IJMRGE.2024.5.1.845-849.

Akhtamova, Y, A. (2023). Protection of consumers under GDPR. The American journal of political science law and criminology, DOI: 10.37547/TAJPSLC/volume05issue08-10.

Alexandre, P., Nicolas, R., & Tracy, S. (2007). Achieving best practices transfer across countries. *Journal of Knowledge Management*, DOI: 10.1108/13673270710752171.

Andreja, P., Gal, P., & Igor, P. (2024). Sovereignty Over Personal Data. Advances in human and social aspects of technology book series, DOI: 10.4018/979-8-3693-3334-1.ch006.

Ashutosh, D. (2024). Cross-Border Data Flows and International Law: Navigating Jurisdictional Complexities in the Digital Age. DOI: 10.36676/IJL.V2. i1.03

Benedicta, E., Ogugua, C., Vivian, A., & Bisola, B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, DOI: 10.30574/wjarr.2024.21.2.0369.

Bernardus, A., Natalia, K., Dennis, B., Michel, E., Kevin, B., & Tobias, F. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Journal of Grid Computing*, DOI: 10.1016/j.giq.2023.101862.

Bhupinder, S. (2024). Cherish Data Privacy and Human Rights in the Digital Age. Advances in human and social aspects of technology book series, DOI: 10.4018/979-8-3693-3334-1.ch007.

Chen, Y., & Jamil, A. (2023). Impact of Enactment of 'The Prevention of Electronic Crimes Act, 2016' as Legal Support in Pakistan. *Academy of education and social sciences review*, DOI: 10.48112/AESSR.V3I2.500.

Christopher, K., Jerker, B., Fred, H., Orla, L., & Christopher, M. (2017). GDPR as a chance to break down borders. *International Data Privacy Law*, DOI: 10.1093/IDPL/IPX023.

Claudia, N., Marius, L., & Camille, S. (2024). Understanding GDPR from requirement engineering perspective—a systematic mapping study on regulatory data protection requirements. *Requirements Engineering*, DOI: 10.1007/s00766-024-00423-4.

Equipe, E. (2022). The Factors Influencing Implementation of Cybersecurity Laws in Developing Economies: *Evidence with Quantitative Analysis*. DOI: 10.31124/advance.20066321.

Eugénie, C., Ans., & Václav, O. (2023). Unraveling cross-country regulatory intricacies of data governance: relevance of legal insights for digitalization and international business. *Journal of international business policy*, DOI: 10.1057/s42214-023-00172-1.

Madiev, F. (2023). Analysis of modern approaches to providing the right to privacy. *Jurisprudence*, DOI: 10.51788/tsul.jurisprudence.3.4. /XSRP3437.

Ferlanda, L., & Armela, M. (2023). Digital Constitutionalism & Data Economy. DOI: 10.1007/978-3-031-60049-4_6.

Graham, G. (2006). New Dimensions in Privacy Law: APEC's privacy framework sets a new low standard for the Asia–Pacific region. DOI: 10.1017/CBO9780511494208.006.

Hazrat, B., & Muhammad, K. (2022). Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective. *Al-Idah*, DOI: 10.37556/al-idah.040.02.0802.

Himani, M., & Suneel, K. (2021). Data protection laws and a comparative analysis of GDPR and PDPB. *Nucleation and Atmospheric Aerosols*, DOI: 10.1063/5.0110597.

Himanshu, K. (2024). Cybersecurity Law: Challenges and Legal Frameworks for Protecting Digital Assets and Privacy Rights. DOI: 10.36676/IJL.V2.I2.05.

Hui, Y., Hui, J., & Tamra, L. (2024). The Cross-jurisdictional Data Transfer in Health Research: Stakeholder Perceptions on the Role of Law. *Asian Bioethics Review*, DOI: 10.1007/s41649-024-00283-8.

Chuang, I., Hsuan, H., & Hwang, Kuo. (2023). An Efficient GDPR-Compliant Data Management for IoHT Applications. DOI: 10.1109/iccworkshops57953.2023.10283547.

Janis, W., Tristan, H., & Kirstie, B. (2022). Data protection for the common good: Developing a framework for a data protection-focused data common. Data & policy, DOI: 10.1017/dap.2021.40.

Jawahitha, S. (2024). Privacy model for the development and implementation of regulatory technology. Journal of infrastructure, policy and development, DOI: 10.24294/JIPD.V8I6.3072.

Kapil, S., Swapnajeet, G., Vikrant, K., Jagadeesh, B., Sanjay, & Adam, P. (2020). Data Sovereignty Governance Framework. DOI: 10.1145/3387940.3392212.

Klaus, E., Jiatao, L., Keith, D., Brouthers, J. & Bryan, J. (2023). International business in the digital age: Global strategies in a world of national institutions. *Journal of International Business Studies*, DOI: 10.1057/s41267-023-00618-x.

Leyland, M. (2005). The impact of trust and reputation on the transfer of best practices. *Journal of Knowledge Management*, DOI: 10.1108/13673270510610350.

Lingjie, K. (2010). Data Protection and Transborder Data Flow in the European and Global Context. European Journal of International Law, DOI: 10.1093/EJIL/CHQ025.

Lubna, D. (2024). Data Security, Privacy and Cyber Policy of Pakistan: A Closer Look. DOI: 10.1109/khi-htc60760.2024.10482125.

Magdalena, S., & Joanna, M. (2023). Between commodification and data protection: Regulatory models governing cross-border information transfers in regional trade agreements. *Leiden Journal of International Law*, DOI: 10.1017/s092215652300050x.

Martina, F., & Erik, M. (2024). Governing personal data and trade in digital services. *Review of International Economics,* DOI: 10.1111/roie.12735.

Miroslav, P., Thomas, R., Chiara, D., Elisa, R., Salvatore, C., & Eugenia, R. (2024). Privacy-Preserving Workflow for Cross-Border Federated Analysis of Data. *Studies in health technology and informatics*, DOI: 10.3233/shti240737.

Monica, T., Caroline, B., Benjamin, L., Michael, K., Hanibal, B., Sven, W., & Tibor, K. (2024). Research collaboration data platform ensuring general data protection. *Dental Science Reports*, DOI: 10.1038/s41598-024-61912-8.

Muhammad, A. H. (2007). Privacy & Islam: From Quran to data protection in Pakistan. *Information & Communications Technology Law*, DOI: 10.1080/13600830701532043.

Musa, M. C. (2021). Privacy and data protection in Europe: Council of Europe Convention 108 and the European Union's GDPR. DOI: 10.4337/9781786438515.00007.

Muslim, A. (2024). Importance of Cybersecurity Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets. *Indian Journal of Public Administration*, DOI: 10.1177/00195561241271520

Namrata, S., & Shallu, B. (2024). Navigating GDPR Compliance: Intersection of Data Governance, Accountability, and OC. International journal of innovative research in engineering & multidisciplinary physical sciences, DOI: 10.37082/IJIRMPS.V12.I4.230875.

Niels, L. (2011). Compliance by design for artifact-centric business processes. DOI: 10.1007/ 978-3-642-23059-2_11.

Olga, I., & Khadzhi, K. (2020). Global Experience in Regulating Data Protection, Transfer and Storage. Economic Policy, DOI: 10.18288/1994-5124-2020-3-152-175.

Pascoal, P., Maria, I., & Isabel, L. (2023). The Implementation of the General Regulation on Data Protection – In the Intermunicipal Community of Douro, Portugal. DOI: 10.1007/978-3-031-44131-8_35.

Pavlo, D., & Ivan, H. (2023). Current challenges and the future of legal protection of personal data: under the influence of digitalization development. *Pravo Ta Innovacii*, DOI: 10.37772/2518-1718-2023-3(43)-12.

Prakhar, G., Cuong, T., Reza, S., & Ferdinando, F. (2024). Data Minimization Principle in Machine Learning. DOI: 10.48550/arxiv.2405.19471.

Rahman, U., Karim, U., & Muhammad, A. (2023). Regulatory constraints, responsibilities and consultation (CRC) for legal institutionalization of cryptocurrencies in Pakistan. *Qualitative Research in Financial Markets*, DOI: 10.1108/qrfm-03-2023-0053.

Rahul, K. (2024). Cybersecurity Law: Challenges and Legal Frameworks for Protecting Digital Assets and Privacy Rights. DOI: 10.36676/IJL.V2.I3.28.

Rana, S., Sayeda, S., & Roshan, S. (2023). The Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to combat Cyber Crime in the wake of CPEC. DOI: 10.31384/*JISRMSSE*/2023.21.4.5.

Randal, B., Zachary, N., & Peterson, J, (2009). Security constructs for regulatory-compliant storage. Communications of ACM, DOI: 10.1145/1629175.1629206.

Rong, C. (2021). Mapping Data Governance Legal Frameworks Around World. Research Papers in Economics, DOI: 10.1596/1813-9450-9615.

Nair, S. (2024). Data protection and constitutional rights: Intersection of privacy and information security. DOI: 10.59126/v3i1a2.

Said, G., & Sherzod, R. (2023). The Personal Data Protection as a Tool to Fight Cyber Corruption. International journal of law and policy, DOI: 10.59022/ijlp.119.

Seema, S. P. (2024). Regulation of cross-border data flow and its privacy in the digital era. DOI: 10.69953/NJRS.V9I2.9.

Svetlana, Y. (2017). Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade Deals" World Trade Review, DOI: 10.1017/S1474745617000453.

Svetlana, Y., & Kristina, I. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. International Data Privacy Law, DOI: 10.1093/IDPL/IPAA003.

Szu, L., Yi-Wen, C., & Yennun, H. (2021). Examining Compliance with Personal Data Protection Regulations in the Interorganizational Data Analysis. Sustainability, DOI: 10.3390/SU132011459.

Tannu, R. (2023). Addressing Cybersecurity and Data Breach Regulations: A Global Perspective. DOI: 10.36676/ijl.2023-v1i1-09.

Tek, R., Anelia, K., Rance, D., Kai, K., & Anna, F. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. Sensors, DOI: 10.3390/s22072763.

Thomas, M. F. (2014). Verbeke, A., International Business Strategy: Rethinking the Foundations of Global Corporate Success, 2nd Edition, Cambridge University Press, 2013. *Management International Review*, DOI: 10.1007/S11575-013-0196-X.

Wang, C. (2021). Analyzing the effects of cross-border e-commerce industry transfer using big data. *Mobile Information Systems*, 2021, 1-12

Wang, Q. (2023). An exploration of the challenges of cross-border data flow for international investment law by counting and fuzzy numerical analysis algorithms. *Applied Mathematics and Nonlinear Sciences*, 9(1).

Xun, P. (2022). Constitutional Basis for Protection of Personal Information. *Journal of Innovation and Social Science Research*, DOI: 10.53469/jissr.2022.09(05).14

Yasar, F., & Mohamed, Z. (2000). Internal transfer of best practice for performance excellence: a global survey. Benchmarking: International Journal, DOI: 10.1108/1463577 0010378882.

Yaseen, T. (2022). Governance enigma: Concerns and human security challenges to Pakistan. *International Journal of Advanced and Applied Sciences*, DOI: 10.21833/ijaas.2022.10.019

Yousra, J., Khond, M., Mohamed, S. (2020). A Study of South Asian Websites Privacy Compliance. IEEE Access, DOI: 10.1109/ACCESS.2020.3019334.

Yujin, K., Ella, C., Gonzalo, M, Chris, H., & Dawn, S. (2023). SoK: The Gap Between Data Rights Ideals and Reality. arXiv.org, DOI: 10.48550/arxiv.2312.01511.

Yuqian, L. (2023). Governance in Free Cross-border Flow Data. Journal of Education, Humanities and Social Sciences, DOI: 10.54097/cq74rw08.

Zerun, Z. (2024). Cross-border Data Flow Governance: The Integration of International Experience and China's Modernization Path. Highlights in business, economics and management, DOI: 10.54097/49 setj81.

Zhongpo, G., Chengwen, K., Xinjian, Z. (2023). The Role and Impact of Cross-Border Data Flows in International Business Digital Trade. Applied mathematics and nonlinear sciences, DOI: 10.2478/amns-2024-2246.