Law and Policy Review (LPR)
Volume 5 Issue 1, Spring 2026
ISSN$_{(P)}$: 2076-5614, ISSN$_{(E)}$: 3007-4290
Homepage: https://journals.umt.edu.pk/index.php/lpr

Check for updates

Title: **A Comparative Analysis of the EU's GDPR and Pakistan's Personal Data Protection Bill, 2023**

Author (s): Muhammad Saleem Javed[1], and Sameer Haider[2]

Affiliation (s): [1]Sukhera Law Chamber, Lahore & Islamabad, Pakistan
[2]Director Child Protection at FIKER, Gilgit-Baltistan, Pakistan

DOI: https://doi.org/10.32350/lpr.51.04

History: Received: February 24, 2026, Revised: March 15, 2026, Accepted: May 16, 2026, Published: June 30, 2026

Citation: Javed, M. S., & Haider, S. (2025). A comparative analysis of the EU's GDPR and Pakistan's personal data protection bill, 2023. *Law and Policy Review*, *5*(1), 64-83. https://doi.org/10.32350/lpr.51.04

Conflict of Interest: Author(s) declared no conflict of interest

A publication of
School of Law and Policy
University of Management and Technology, Lahore, Pakistan

Data Protection: A Comparative Legal Analysis of the European Union's GDPR and Pakistan's PDPB 2023

Muhammad Saleem Javed[1]* and Sameer Haider[2]

[1]Sukhera Law Chamber, Lahore & Islamabad, Pakistan
[2]FIKER, Gilgit-Baltistan, Pakistan

Abstract

This paper compares and contrasts General Data Protection Regulation (GDPR) of the European Union and Pakistan's Personal Data Protection Bill (PDPB) 2023, with respect to their legal foundations, scope, rights of the data subjects, enforcement provisions, and the regime of cross-border data transfer. Using a qualitative approach to doctrine, the study examines how both legal frameworks address contemporary privacy issues and govern the processing of individual data in a growing interconnected digital world. The analysis finds that while the GDPR is an advanced rights-focused framework based on the core EU principles, the PDPA 2023 in Pakistan is an emerging framework influenced by international standards but shaped by national security and sovereignty considerations. The study identifies several similarities between the two frameworks, including the recognition of core data subject rights and the requirement for lawful and transparent data processing. However it also highlights significant differences especially on regulation independence, data localization requirements, adequacy evaluation, and the balance of state power and personal privacy. The study concludes that although the Personal Data Protection Bill 2023 incorporates several features of the GDPR, its limitations on cross-border transfers and the wide discretion authorities given to the government in the exercise of its powers may be problematic for effective implementation. To build an effective and rights-based data governance regime in Pakistan, institutions need to be able to have autonomy and interoperability with the rest of the world.

***Keywords*:** data protection, GDPR, Pakistan, privacy, personal data protection

Introduction

The General Data Protection Regulation (GDPR), which is now effective since May 2018, is a landmark legislation of the European Union (EU) on

*Corresponding Author: info@slc.com.pk

privacy and personal data protection. It creates a comprehensive legal framework, including a wide range of rights for data subjects and robust duties for the data controllers and processors. The GDPR's impact on the world makes it a standard for other jurisdictions looking to update their data protection regulations. In response to this global phenomenon, Pakistan has taken a bold step in creating a dedicated legislative structure for the protection of personal data, with the enactment of the renowned Personal Data Protection Bill 2023 (Durrani, 2023). The advent of Bill acknowledges that the existing legal framework in Pakistan was not sufficient in the context of the rising problems created by the digital economy and the processing of personal information. Before the proposed legislation, there was no comprehensive data protection statute, the issues of data protection and informational privacy were dealt with under a 'sectoral' regulatory framework involving primarily sectoral regulatory instruments and the cybercrime legislation including the Prevention of Electronic Crimes Act, 2016 (PECA) (Malik, 2022).

The Constitution of the Islamic Republic of Pakistan, at the constitutional level, provides for the inviolability of the dignity of man and the privacy of the home in Article 14 of the Constitution. Pakistani Courts have taken a liberal interpretation of Article 14 and have extended the right to personal privacy to the digital realm, even though there is no explicit mention of this right in the Constitution. In the case of Rawalpindi v. District Bar Association (PLD 2015 SC 401), the Supreme Court highlighted that privacy, human dignity, and personal liberty are fundamental constitutional values which must be given strong protection through law. However, Pakistan has not had a comprehensive law on the collection, processing, storage, disclosure, and trans-border transfer of personal data in the past, despite these constitutional safeguards. Therefore, privacy issues were mainly solved by PECA 2016 and other sector-specific legislation, which created an inconsistent and fragmented regulation regime.

In this context, the Personal Data Protection Bill, 2023 is the country's first comprehensive legislation aimed at creating a comprehensive data protection framework. This part hence explores the similarities and differences between EU's existing GDPR system and the new data protection law in Pakistan, focusing on the principles and processes of personal data protection, privacy rights, and data processing operations.

Literature Review

Personal data has become a significant economic and social asset, and its massive growth has raised many questions about privacy, surveillance, and informational self-determination. Today, the importance of data protection is more and more acknowledged as a human right, rather than just a regulatory issue. In Europe, privacy and data protection have become separate but related rights and the GDPR has been developed as a broad, all-encompassing legislation to govern the collection, processing, and sharing of personal information. Proponents say that today's data protection legislation aims to balance the individual rights of privacy with the economic advantages of the digital economy. The GDPR is often referred to as the most impactful regulatory model in this context and sets high standards of accountability, transparency and user control over personal information.

The GDPR has received a great deal of attention in academic publications, with particular emphasis on the GDPR's rights-based approach, enforcement powers, and extraterritorial effect. Paul Schwartz has written about issues of transatlantic data governance, while other scholars have been looking at how increasingly cross-border data flows are being addressed through international cooperation and by regulating data (Schwartz, 2019). Likewise, Christopher Kuner has pointed to the GDPR's contribution to the global privacy norm and the impact it has had on privacy legislation outside of Europe. Other experts have focused on the innovative aspects of the regulation such as the rights of access, rectification, erasure and data portability (Kuner, 2020). The GDPR is considered to be a game-changer piece of legislation that has reshaped the rights of individuals, the role of corporations, and the power of states in the digital era. However, difficulties in compliance costs, regulatory fragmentation and different implementation across Member States have also been noted.

The impact of the GDPR extends well beyond Europe and has inspired the development of data protection regulations across Asia, Africa and Latin America. As Graham Greenleaf notes, In recent years, there has been a growing global trend among jurisdictions to enact privacy legislation aligned with international standards while adapting it to their respective political, economic, and cultural contexts (Greenleaf, 2021).

Countries in Asia, including India, Singapore, South Korea and Japan,

have enacted data protection rules that offer a more holistic framework for data protection, blending international privacy principles with domestic regulation interests (Kuner, 2020). Past research has focused mainly on the disjointedness of the current privacy regime, which has historically been based on constitutional safeguards, sectoral laws and the laws pertaining to cybercrime, including the Prevention of Electronic Crimes Act 2016 (PECA). The lack of a data protection law has left the collection, storage, and transfer of personal data in a legally precarious situation.

The Personal Data Protection Bill 2023 has attracted considerable attention for its compliance with international standards, notably the GDPR. Although the Bill contains many data-subject rights and regulatory principles that are well understood in the international community, some issues have been raised about its blanket exceptions for government authorities, regulatory autonomy, and its limiting cross-border data transfer provisions. The Bill has been given special attention for its data localization provisions that have been seen to pose certain challenges to digital trade, foreign investment and technological innovation by some commentators. Although there is a vast amount of literature available on data protection and privacy regulation, few scholars have conducted a detailed comparison between GDPR and Pakistan's Personal Data Protection Bill 2023. Discussions currently underway tend to be confined to either the GDPR as a model one way to regulate or descriptive programmes of Pakistan's proposed framework. This means that there is a lack of literature on how both instruments differ in important aspects like regulatory independence, data-subject rights, enforcement and cross-border data governance.

This study aims at answering the following research question: What are the legal, institutional and policy differences and similarities between GDPR of European Union and Personal Data Protection Bill 2023 of Pakistan that could impact the implementation of this legislation and the interoperability of the privacy regulations? The paper seeks to answer this question and helps to fill the growing jurisprudence concerning comparative data protection law and offers an insight into the issues that developing jurisdictions have to face if they want to implement globally recognised data protection standards.

Methodology

The study adopts doctrinal and qualitative research methodology to analyse

and compare the General Data Protection Regulation (GDPR) of the European Union with Personal Data Protection Bill 2023 (Durrani, 2023) of Pakistan. Doctrinal legal research is especially appropriate for comparative legal analysis because it involves the systematic study of law, legislation, judicial decisions and regulations. The study assesses the substantive provisions, institutional systems, enforcement mechanisms and policy goals of both instruments and draws conclusions about any areas of similarity and/or differences. A functional approach to the comparative analysis is used. Both GDPR and PDPB 2023 are analysed through the common criterion (tertium comparationis): effectiveness of the protection of personal data and of the rights to privacy of individuals in the digital environment.

This study primarily relies on authoritative legal sources as the foundation of its analysis. Primary sources consist of the text of the Regulation (EU) 2016/679 (GDPR), the Pakistan Personal Data Protection Bill 2023, official policy documents, and some judicial decisions related to privacy and data protection. Other secondary sources include books, academic journal articles, publications by international organizations, legal commentaries, and policy reports. To ensure analytical balance, this study relies primarily on primary legal texts as authoritative sources, while secondary literature is employed to provide contextual interpretation, theoretical insights, and scholarly critique.

Special focus is paid to literature covering privacy rights, cross-border transfers, regulatory independence and data localization policies. The study centers on five key aspects of comparison: Legal foundations and policy goals; Rights of data subjects; Regulatory authorities and design of institutions; Enforcement mechanisms and sanctions; Cross-border data transfers and implementation issues. Such dimensions were chosen as they encompass the fundamental aspects of modern data protection systems, and have a direct impact on the effectiveness of privacy regulation. There are some limitations of the study. The GDPR is a law that is already in full effect and has been implemented for several years, while PDPB 2023 is still a draft and has yet to be put into practice. Hence, the discussion of the Pakistani framework is more of a prediction than an observation. Secondly, the study is mainly doctrinal and legal in nature, and lacks empirical data collected from interviews, surveys and/or stakeholder consultations. Lastly, the dynamic and fast-changing nature of digital governance and privacy

laws is likely to shift the comparative picture discussed in this paper in the future.

Legal Foundations

The GDPR and the PDPA 2023 are based on fundamental principles of privacy and data protection rights. These are based in the EU on Article 16 of the Treaty on the Functioning of the European Union, and in Article 8 of the EU Charter, which specifically provides the right to the protection of personal data. The GDPR is an applicable EU Regulation in its own right-Regulation (EU) 2016/679 -which replaces the previous Data Protection Directive of 1995. It aligns data protection regulations throughout the Union, and directly proposes to safeguard the rights of individuals as well as free movement of data across the inner market (Chambers and Partners, 2025). The GDPR provides general legal grounds of processing (including consent, contract or legitimate interests) (Arts 6 7), and severe requirements of special categories of data (Art 9). These goals (according to Recital 5) are strengthening the basic rights to protection of information and privacy, and the harmonization of regulations to enable the digital economy (Bygrave, 2014; Lynskey, 2015).

In Pakistan, the PDPA 2023 is still at the bill stage but has been approved by the federal cabinet and forwarded to Parliament without public consultation (European Union, 2016). It appears modelled substantially on the GDPR, as it even uses similar terminology (e.g. “data controller/processor”, “sensitive personal data”, “data subject”, etc.). The Bill’s preamble and provisions invoke the government’s duty to protect citizens’ privacy and personal data, yet they also contain broad exemptions for public authorities and national security interests (e.g. under “public interest” and “legitimate interest” grounds). This mirrors a tension in many jurisdictions between privacy rights and state powers. Unlike the GDPR, which is founded on explicit EU treaty competence in Article 16 TFEU, the PDPA’s legitimacy rests on the ordinary legislative powers of Pakistan’s federal parliament and the implied constitutional right to privacy (Malik, 2022).

The GDPR emerged in a well-established supranational regulatory context, where both regulatory institutions and bodies and judicial oversight are fairly developed. Unlike the PDPB 2023, which is aimed at creating a full-fledged privacy regime in a jurisdiction where data protection is still a

fledgling field of law, the legislation in Southern Africa is relatively rudimentary. Therefore, the similarities in legislative drafting do not necessarily mean that there will be similar results in practice.

Rights of Data Subjects

The GDPR and PDPA 2023 both enumerate extensive rights for individuals (data subjects) regarding their personal data. Under the GDPR (Arts 12–23), data subjects have rights of access, rectification, erasure ("right to be forgotten"), restriction of processing, objection, data portability, and a right not to be subject to decisions based solely on automated processing (including profiling). It also imposes duties on controllers to inform subjects about processing activities, and on processors and controllers to assist in facilitating these rights.

The PDPA 2023 mirrors most of these rights in its own chapter on "Rights of Data Subjects". For instance, Section 16 of the PDPA gives a data subject a right of access to his or her personal data held by a controller, including confirmation whether data concerning the subject is being processed, and (on payment of a nominal fee) a copy of the data (European Union, 2016). This contrasts with the GDPR, which requires that access be provided free of charge (Art 12(5)). Section 19 provides a right to correction (rectification) of inaccurate data, and Section 26 grants a right to erasure without undue delay, closely resembling GDPR Article 17. Likewise, Section 29 of the PDPA affords the right to data portability and includes the GDPR-style safeguard that a subject shall not be subject to a solely automated decision causing legal or similarly significant effects unless he has given explicit consent (Chambers and Partners, 2025). Both regimes therefore recognize the modern rights to data portability (transferring one's data between controllers) and to contest automated profiling (compare GDPR Art 20 and 22).

Nevertheless, there are differences in detail. The PDPA requires written requests for certain rights and even allows a processing fee, whereas the GDPR emphasises simple, prompt and free access. For example, under Section 16(3) of the PDPA an access request incurs an "administrative" fee (Ministry of Information Technology and Telecommunication [MITT], 2023), whereas Art 15(3) GDPR bars such charges (save in exceptional circumstances). Similarly, while the GDPR explicitly provides a free "right to be forgotten" with limited exceptions, the PDPA's erasure right is subject

to certain lawful-processing exceptions (e.g. for public interest or legal claims)– they are both generally very similar in terms of the list of exceptions (national security, public interest, etc). Another new feature of the PDPA is the explicit enumeration of types of sensitive personal data (including health data, religion, biometrics, caste, etc) that are to receive increased protection. This mostly coincides with the special categories (race, health, religion etc.) of the GDPR, however, such additions as the caste or national ID numbers are specific to the Pakistani context. In a nutshell, the Bill tries to estimate the basic user rights of the GDPR with other bureaucratic conditions (fees) and exemptions that may narrow their terms (Greenleaf, 2021).

The PDPB 2023 includes some rights that have been recognised under the GDPR, but there are also some procedural restrictions such as the potential for administrative fees and the overarching statutory exceptions which may impact on the ease with which these rights are accessible. Data protection regimes are only as effective as the ability of people to use their rights, whether or not those rights are formally recognised (Greenleaf, 2014).

Regulatory Authorities

Under the GDPR framework, each EU Member State must establish one or more independent Data Protection Authorities (DPAs) responsible for monitoring the law's application (European Union, 2016). The GDPR (Arts 51–52) requires these authorities to be independent, staffed with adequate resources, and to cooperate with one another and the European Data Protection Board (EDPB) as needed. In practice this has created a network of national regulators (e.g. the UK ICO, French CNIL, etc.) that enforce GDPR compliance domestically, with mechanisms for cross-border cooperation (the "one-stop-shop" for cross-border controllers via a lead authority). For example, GDPR Article 52 expressly mandates that "each supervisory authority shall act with complete independence" in exercising its functions (European Union, 2016). Thus, the EU model anchors data protection enforcement in autonomous agencies with legal powers to investigate, advise and sanction

By contrast, the PDPA 2023 concentrates regulatory power in a newly created National Commission for Personal Data Protection (NCPDP). Section 35 of the Bill requires the federal government to establish this

Commission, consisting of a chairperson and four members appointed on the government's recommendation. More importantly, the Commission is constituted as an independent body that is under the administrative control of the Federal Government (MITT, 2023). This would probably require its budget and leadership to be dependent on the executive. These critics of surveillance have cautioned that a system like this will undermine the impartiality of the authority (Privacy International, 2023). In fact, the absence of an independent appointment procedure has been mentioned as one of the most significant flaws of the Bill: e.g., despite the opponents of the law, even inaccurate rules and unspecified exceptions of the public interest, coupled with the regulator operating under governmental control, may serve as a source of executive discretion.

The powers of the Commission formed under the PDPA would be broad once formed. It may listen to complaints, make investigations, make enforcement decree and even suspend or make data processing registration. To illustrate, when the Commission discovers a violation it has the authority to impose fines of up to USD 2,000,000, suspend/terminate the registration of a violator (European Commission, n.d.). It can also impose up to 1 per cent of annual revenue of a company as the top of penalties (MITT, 2023). These design options revere the GDPR strategy of stringent regulatory control, but in Pakistani law they are entrenched in one national institution instead of a multiplicity of independent DPAs. Overall, the PDPA places a central regulatory body with comparable powers to the EU regulators, albeit arguably less formally isolated against government pressure.

One of the biggest differences between the two is the regulatory independence. While the supervisory authorities under the GDPR have a high degree of institutional independence, there have been concerns about the extent of executive influence in the proposed regulatory framework in Pakistan. More independence could build public confidence, strengthen the credibility of the regulatory system and also improve the recognition of the Pakistani regime by the international community (Greenleaf, 2014).

Enforcement Mechanisms

Both the GDPR and the PDPA have severe penalties for non-compliance but the amounts vary. According to Article 83 (5) of GDPR, the administrative fines for the severe violations of GDPR may be up to €20 million or 4% of the total annual turnover of the undertaking, whichever is

higher, worldwide in the previous financial year. These include breaches to the basic principles of data processing, data subject rights, and international transfer of data. The high level of these fines demonstrates the GDPR's principle that enforcement shall be "effective, proportionate and dissuasive" throughout the EU. The GDPR itself outlines an administrative enforcement regime, but under Article 84, Member States can have more stringent rules on penalties, including criminal penalties if applicable. As a result, while there is no direct criminal liability under the GDPR, some Member States have added domestic measures to the Regulation, covering serious violations of data protection (Asad & Irfan, 2025).

Under the PDPA 2023, enforcement takes both penal and regulatory forms. Several acts of "unlawful processing" are criminalized with monetary penalties but no custodial sentence. Section 48, for instance, sets graduated fines: up to USD 125,000 for a single violation, doubled for repeat offenses; and substantially higher fines (up to USD 500,000 or 1,000,000) if the data is sensitive or critical (MITT, 2023). Separate provisions impose smaller fines (e.g. up to USD 50,000 for failure to implement security measures, or for defying a Commission order. These penalties apply to natural persons; companies ('legal persons'), under Section 50(5), face fines up to 1% of turnover or USD 200,000 (whichever is higher). Moreover, unlike the GDPR where only courts impose punishments in most Member States, the PDPA empowers the Commission itself to impose some fines administratively (MITT, 2023).

Regarding the style of enforcement, both regimes make use of money finances and official decrees. One difference is their magnitude: the maximum fines under the GDPR are by a whole order of magnitude larger (millions of euros or up to 4% of global revenue) than the maximum fines imposed by the PDPA on individuals (USD 1 million) and on companies (which is practically limited to 1% of Pakistani turnover, which might be much less than global revenue). Conversely, the PDPA proscribes some data offenses directly (although only fines are provided); the GDPR does not impose criminal responsibility directly (it is an administrative regime under EU law, but the member states may qualify crimes). The PDPA also makes the Commission a civil court, which has substantial investigatory authority (including search and seizure of evidence) (MITT, 2023) an approach reflected in certain jurisdiction data laws. On the whole, both systems are supposed to vigorously prevent breaches, but enforcement of

the GDPR is based on transnational corporate compliance (large multinationals would face big fines) whereas the approach used in Pakistan appears to focus on the deterrence effect of both criminalizing abuse and giving its national regulator more power.

The different enforcement mechanisms illustrate the different priorities of the regulators. While the GDPR is based on a principle of "deterrence" with significant penalties for administrative misconduct and active oversight, the PDPB 2023 focuses more on compliance within a nascent institutional framework. Ultimately, however, the capacity and independence of the authority for implementation will be key to effective enforcement (Asad & Irfan, 2025).

Challenges in Implementation

Both jurisdictions face difficulties when trying to implement data protection law in practice; however, of another nature. The standardized nature of the GDPR has in practice been cut by national interpretations in the EU, with calls to provide more guidelines and resources to enforce it. Indicatively, various observers observe that most DPAs are overworked and that the new requirements (like mandatory breach reporting and consent requirements) have placed heavy compliance costs on businesses (Thomson Reuters, n.d.). It has been also criticized that the rules are not uniformly applied by all Member States, and that rights (such as rights of access requests) are frequently exercised much less frequently than anticipated. The extraterritorial nature of the GDPR (including non-EU processors) has provoked controversy regarding the coordination of its application across the world. Briefly, the compliance of GDPR in the EU is still in the process of completion; however, in five years, it has been thoroughly fixed in the life of law and business.

In Pakistan, the PDPA is confronted with very different challenges. To begin with, there is a deficiency of previous data protection experience, and thus little precedent or infrastructure. Individuals are very ignorant of their rights, and governments and businesses are mostly unaware of their new duties. According to Pakistani commentators, privacy is significantly below the global norms in Pakistan because of low awareness and ineffective enforcement (Asad & Irfan, 2025). The attitude of the government itself has become worrying: Privacy International points out that the Bill has sweeping exceptions in the form of national security and the public interest,

which are so poorly defined, as to almost devour most rights, in light of the questionable independence of the Commission (Privacy International, 2023)

The next issue of concern is data localization and cross-border aspects of the Bill. The PDPA, much like the majority of the so-called GDPR-like laws in Asia, categorizes data (ordinary, sensitive, critical) and is well-regulated. The Bill provides that any critical personal data shall be processed on the servers located in Pakistan, and even sensitive data may need a local storage or governmental authority to transfer it (Information Technology and Innovation Foundation [ITIF], 2025). Whereas the GDPR allows transfers to sufficient countries, or protects, the test of adequacy in the PDPA is not clearly defined, and authorities have broad discretion. Critics are concerned that such a localization policy will increase the cost and create a fractured Pakistani digital economy: not only will it require foreign companies to install their data centers in Pakistan, it will also limit cross-border services, damaging Pakistani companies competing internationally (ITIF, 2025). As a matter of fact, industry players have cried foul that the Bill fails to take into account their advice that the Bill can not be used to impose too much compliance cost and data-flow burdens that would discourage growth in the Pakistani tech industry (Younus, 2023).

Overall, although both laws focus on robust enforcement, the PDPA in Pakistan is facing state capacity, stakeholder buy-in and technological infrastructure challenges of implementation. The EU on the contrary is struggling with the fine-tuning of its implementation and the uniformity of enforcement across different societies. Pakistan will have to construct new institutions (the Commission), train regulators and educate the people and businesses. It has been called upon that Pakistan adopts a more consultative drafting process; one commentator cries foul that it could be passed with haste without involving stakeholders creating a law that is both onerous and poorly targeted (Younus, 2023). Eventually, the success of the PDPA will hinge on whether Pakistan can create true independence of its regulator and offer clear regulations, and not just on the paper requirements which replicate the GDPR (Asad & Irfan, 2025).

Legislative reform alone is unlikely to ensure effective data protection. Public awareness, institutional expertise, technological capacity, and regulatory resources will play a decisive role in determining whether the objectives of the PDPB 2023 can be translated into practical protection for

data subjects.

Cross-Border Data Transfers and Digital Trade Implications

Article 44-50 of Chapter V of GDPR provides that information can only move out of the EU when the required protection is provided. Article 44 states that any personal data transfer to a third country or international organisation shall occur only when it has been established that the conditions provided in this Chapter are met (Malik, 2022). The GDPR thus assumes free movement of data with protection, rather than the banning. They can transfer on the basis of an adequacy decision (Article 45) or on suitable safeguards (Article 46). On the contrary, the PDPB 2023 in Pakistan is explicitly protective. The Bill divides the data into the following levels regular, sensitive, and critical and enforces strong localization. Personal data of critical nature should only be handled in Pakistani servers (Younas, 2023). Transfers are also allowed in the case of other data provided that the receiving country provides a regime that is at least comparable to the one of Pakistan and subject to the conditions by the new Data Protection Commission (NCPDP). Therefore, EU law promotes border flows on a conditional basis, but the PDPA regulates conditional flows based on Pakistani sovereignty and security interests (Aaronson, 2021).

Article 45 of GDPR stipulates that an adequate level of protection is assessed by the European Commission under criteria including the rule of law, basic rights and the existence of efficient protection mechanisms (Privacy International, 2023). A finding of adequacy (e.g. in the case of UK, Japan, Canada, etc.) permits transfers without additional protections as though the data stayed in the EU (Khan, 2025). These determinations are reviewable and subject to revocation (as was the case with the EU-US Privacy Shield that was struck down and replaced by the EU-US Data Privacy Framework). Practically, the standards that the Commission has rigorously adopted have been adopted in only a few jurisdictions on adequacy decisions. Without adequacy, Article 46 of the GDPR only allows transfers where the controller offers appropriate safeguards (e.g. Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes of conduct or certification mechanisms), and ensures enforceable rights to data subjects. As an example, specific authorisation is not required when using legally binding SCCs or BCRs (MITT, 2023). Both as a backup (Article 49), transfers can be made only under the strictest derogations, including the express permission of the data subject or performance of

another contract.

In comparison, the recent PDPA 2023 (in the draft phase) is even more restrictive. It states that no personal information should be sent to a foreign country unless the destination country has offered the same protection as that by Pakistani law (European Union, 2016). This in practice implies that the NCPDP needs to find a way of establishing whether the laws of any country are robust enough. Otherwise, the transfers can only take place on certain conditions: in case of a binding contract, explicit consent (varying with national security), international cooperation, or any other conditions may be mentioned by the Commission. Most importantly, important personal information is strictly forbidden to go outside of Pakistan. The Bill also stipulates that the NCPDP should establish a mechanism that will make sure that some elements of sensitive personal data are still in Pakistan (MITT, 2023). These localization requirements are stronger than the GDPR, and indicate that there will be a focus on national sovereignty in digital space and national dominance over data. In a few words, even though the GDPR mandates a homogenous and high protection level of any transfer, the PDPA places a special domestic filter: the flow of data may not pass without the approval of the Pakistani authorities or without strict conditions.

Comparatively, the EU strategy focuses on mutual realisation of protections and contractual/organisational instruments, whereas Pakistan is focused on jurisdictional containment. To the EU, Article 45 adequacy or Article 46 safeguards is the key, without either of them, transfer is possible only by way of narrow provisions (Article 49). In the case of Pakistan, the most important test is the equivalent level of protection which is defined by the NCPDP. Both regimes put a nominal adherence to an adequacy-like mechanism; however, they are organized differently and with different priorities. The GDPR offers a unilateral mechanism of adequacy in a multilateral manner (Commission proposal, EDPB opinion, Council vote) (Jutte, 2024), (PDPA leaves the standards purely to the national regulator and even hypothetically proposes potentially ambiguous standards). Similarly, SCCs/BCRs approved under GDPR can offer established pathways to compliance, whilst the Bill in Pakistan does not reference any sort of safe harbour tool; instead envisioning a broad-based regime based on a binding contract/agreement regime. Effectively, the EU gives businesses the guarantee that transfers are legal as long as Chapter V requirements are fulfilled, whereas the PDPA provides a more lenient

approval system.

The digital trade and sovereignty implications are also divergent. In its trade strategy, the EU specifically connects the free cross-border data flows with economic growth. The research service of the European Parliament notes that free movement of data is essential in economic development and may augment the gains of digital trade. Therefore, a digital trade chapter is present in all contemporary EU trade agreements and prohibits unreasonable limitations on the flow of data (including data localization) and encourages interoperability. According to the Commission, it aims to demonstrate that a high standard of data protection and facilitation of cross-border trade can be complementary to each other (Jutte, 2024). This in practice would allow EU businesses to transfer personal data to numerous partners on a single framework of rights, and even the WTO e-commerce talks seek to enshrine the freedoms of data flows to trade. The PDPA of Pakistan, in its turn, represents a more protectionist or sovereignty-oriented model. It sets up clear obstacles which would otherwise be not justified within EU trade standards, such as an EU digital partnership would prohibit data localization. In fact, according to one analysis, the Pakistani law is a source of a disjointed digital order by advancing a data governance model that is based on sovereignty rather than openness (Malik, 2022). This disintegration contradicts the aim of the EU interoperability of global data markets.

The differences between the GDPR and the PDPB 2023 regarding cross-border transfers show two contrasting approaches to regulation. The GDPR emphasises the free flow of personal data and sets the necessary level of protection in place with tools like adequacy decisions, standard contractual clauses, and binding corporate rules. The PDPB 2023 is a more measured approach, with more flexibility in government decision making regarding transfers of data abroad, and a focus on national control of data flows. This might enhance the national security goals and data sovereignty, but could also pose compliance challenges for businesses, hinder international interoperability, and limit Pakistan's involvement in the digital economy. Therefore, the enforceability of the PDPB's transfer regime will rely on the possibility of the regulation's adjustments with commercial and technological realities (Greenleaf, 2021).

Conclusion

This research has compared and contrasted the Personal Data Protection Bill 2023 of Pakistan with EU's General Data Protection Regulation (GDPR). The analysis demonstrates that there's a significant amount of overlap between the PDPB 2023 and the GDPR's core principles, like conditions under which processing is considered lawful, rights of the data subjects, measures of accountability, and regulatory oversight. These similarities suggest that Pakistan's proposed data protection framework has been designed to align with internationally recognized standards and best practices.

Despite these similarities, the study also identifies significant differences between the two legal frameworks. The GDPR is embedded within a comprehensive institutional framework. with strong enforcement and international data transfer mechanisms, and independent supervisory bodies. The PDPB 2023, on the other hand, still has reservations about the independence of the regulators, the wide discretion in the hands of governments, and the restrictions on cross-border data transfers. The differences are not only technical, they are likely to impact the effectiveness, credibility and international interoperability of Pakistan's future data protection regime.

Moreover, the comparison shows that the real problem of Pakistan is not the implementation of the substantive rights but the effective implementation of the rights. Institutional capacity, expertise of the regulatory bodies, awareness and knowledge of the public, judicial support and independence and transparency of enforcement institutions will be key factors of the success of the Personal Data Protection Bill, 2023 (Durrani, 2023). In addition to the statutory protection of privacy and personal data, such institutional safeguards are essential to complement it, because a clear and strict legal framework is not enough to guarantee the effective protection of personal data and privacy rights.

Data transfers across the borders also suggest a greater policy issue in many developing states. New measures for data-localisation and government regulations could also help national security and sovereignty interests, while reducing digital trade, foreign investment, technological innovation and cross-border data transfers. Thus, finding a right balance between privacy protection and economic integration will be essential to the

long-term success of Pakistan's data governance framework.

Overall, the PDPB 2023 is a positive step towards modernizing Pakistan's privacy and data protection regime. The legislation should be GDPR compatible, but should not be a legislative end in itself. Moving forward, institutional independence, development of cross-border transfer mechanisms, improved stakeholder engagement and awareness need to be enhanced to ensure that a rights-based and internationally compatible framework for data protection is built up to address the challenges of the digital age.

Author Contribution

Muhammad Saleem Javed: conceptualization, methodology, investigation, data curation, formal analysis, visualization, writing – original draft, writing – review & editing. **Sameer Haider:** validation, resources, writing – review & editing.

Conflict of Interest

The author of the manuscript has no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data supporting the findings of this study will be made available by the corresponding author upon request.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not use any type of generative artificial intelligence software for this research.

References

Aaronson, S. A. (2018). *Data is different: Why the world needs a new approach to governing cross-border data flows* (IIEP Working Paper 2018-10). Institute for International Economic Policy, George Washington University. https://iiep.gwu.edu/data-different-why-world-needs-new-approach-governing-cross-border-data-flows

Asad, A., & Irfan, D. (2025). Data privacy loss in Pakistan as compared with other countries' security policies and laws (EU GDPR). *Kashf Journal of Multidisciplinary Research*, *2*(3), 138–150. https://doi.org/10.71146/kjmr346

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press. https://doi.org/10.1093/

acprof:oso/9780199675555.001.0001

Chambers and Partners (2025). *Data protection & privacy 2025: Pakistan*. Global Practice Guides. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/pakistan

Durrani, F. (2023, August 10). *Personal Data Protection Bill 2023: Safeguarding privacy in Pakistan*. The Nation. https://www.nation.com.pk/10-Aug-2023/personal-data-protection-bill-2023-safeguarding-privacy-in-pakistan

European Commission (n.d.). *Digital trade*. Trade and Economic Security. Retrieved February 22, 2026, https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en

European Union. (2016). 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199679669.001.0001

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, *169*, 1, 3–5. https://doi.org/10.2139/ssrn.3836348

Information Technology and Innovation Foundation. (2025, May 16). *Pakistan's cross-border data transfer regulation*. https://itif.org/publications/2025/05/16/pakistan-cross-border-data-transfer-regulation/

Jütte, M. (2024). *The EU's digital trade policy*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757615/EPRS_BRI(2024)757615_EN.pdf

Khan, S. (2025, July 21). *Pakistan: Data protection laws and regulations 2025*. International Comparative Legal Guides. https://iclg.com/practice-areas/data-protection-laws-and-

regulations/pakistan

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Malik, O. I. (2022, July 4). *Right to privacy*. Dawn. https://www.dawn.com/news/1698120

Ministry of Information Technology and Telecommunication. (2023). *Draft of the Personal Data Protection Bill, 2023*. https://www.icnl.org/wp-content/uploads/Personal-Data-Protection-Bill-2023.pdf

Privacy International (2023, August 8). *Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill*. https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data

Schwartz, P. M. (2019). Global data privacy: The EU way. *New York University Law Review*, *94*(4), 771–818.

Srivastava, A. (n.d.). *Data localisation in South Asia*. DCU Law and Tech. https://lawandtech.ie/data-localisation-in-south-asia/

Thomson Reuters. (n.d.). *Top five concerns with GDPR compliance*. Retrieved February 22, 2026, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

Younus, U. (2023, July 26). *Pakistan needs to press pause on its data overhaul*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/pakistan-needs-to-press-pause-on-its-data-overhaul/