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

Title:	**Data Protection in the Age of AI: A Legal Analysis of the Impact of Foreign Data Protection Laws on Pakistani Businesses**
Author (s):	Syed Suliman Ali, Nazli Ismail Nawang and Mohd Badrol Bin Awang
Affiliation (s):	Universiti Sultan Zainal Abidin, Terengganu, Malaysia
DOI:	https://doi.org/10.32350/lpr.51.06
History:	Received: January 08, 2025, Revised: December 30, 2025, Accepted: March 28, 2026, Published: June 30, 2026
Citation:	Ali, S. S., Nawang, N. I. & Awang, M. B. B. (2026). Data protection in the age of AI: A legal analysis of the impact of foreign data protection laws on Pakistani businesses. *Law and Policy Review*, *5*(1), 106–127. https://doi.org/10.32350 /lpr.51.06
Copyright:	© The Authors
Licensing:	This article is open access and is distributed under the terms of Creative Commons Attribution 4.0 International License
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 in the Age of AI: A Legal Analysis of the Impact of Foreign Data Protection Laws on Pakistani Businesses

Syed Suliman Ali, Nazli Ismail Nawang*, and Mohd Badrol Bin Awang

Faculty of Law and International Relations, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia

Abstract

Data protection is one of the critical concerns for small and medium-sized enterprises (SMEs) in Pakistan in the context of the dynamic global digital economy. This research explores the complexities of enforcing foreign data protection laws in the international arena, specifically with respect to extraterritorial coverage of the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The main contribution of the study is the documentation of the troubles faced by Pakistani SMEs that are seeking to transfer data across borders, notwithstanding the challenges of conflicting legal obligations imposed on them for such a transfer. The paper then conducts qualitative analysis, including case studies on successful Pakistani SMEs, which help identify successful legal strategies, including the use of Standard Contractual Clauses (SCCs), Data Transfer Impact Assessment (DPIA) and the development of robust privacy policies. The results highlight the importance of good planning, employee training, and partnerships with industry professionals to obtain compliance in addition to improving data security. In addition, the research stresses the importance of having a comprehensive national data protection framework set in place to keep pace with international standards and help encourage SME compliance. This paper seeks to provide actionable recommendations and insights to Pakistani organizations to protect them against the complexity and rigor of data protection regulations and to help them become operationally resilient in the global market.

***Keywords*:** data protection, small and medium-sized enterprises, cross-border data transfers, general data protection regulation, compliance strategies, standard contractual clauses, data transfer impact assessment

Introduction

In today's current global digital economy, data protection has become a

*Corresponding Author: inazli@unisza.edu.my

significant issue in business and the nation. With ever more commerce, communication, and information dissemination occurring on digital platforms, it is now more than ever imperative to protect personal and sensitive information. The digital landscape is home to a variety of businesses, which can mean that they are dealing with many data that they have to protect and, increasingly, their interactions across borders. Understanding the legal frameworks on which data protection rests becomes essential given the rapid flow of data across borders and the ever-changing regulatory environment in countries such as Pakistan (Santema & Kempenaers, 2023).

The global economy relies on cross-border data flows to enable its functioning, from supporting international trade and allowing businesses to operate efficiently to driving innovation by bringing together various sources of data. However, cross-border data transfers are more complicated by the cross-border existence of different data protection laws. Companies across the world are being forced to raise their game in terms of personal data management owing to the European Union's General Data Protection Regulation (GDPR). Moreover, Pakistani businesses, in particular, encounter major difficulties in fulfilling requirements under foreign data protection laws with extraterritorial scopes, which are unlikely to be compliant with local laws (Junejo et al., 2023).

Foreign data protection laws present a number of legal challenges for Pakistani businesses with respect to their extraterritorial application. These are conflicting legal requirements and implications, including penalties for non-compliance and other compliance expenses. In addition, the lack of a defined data protection framework in Pakistan, where no definite data protection framework exists, puts businesses in a legal and operational quandary where transactions are liable to ambiguous dispositions and discontinuities. With the growth of the digital economy, Pakistani businesses must be aware of the consequences of foreign data protection regulations and formulate strategies to address the associated risks (Abdelkarim, 2024). This study seeks to answer several important questions: What is the foreign persistence of data protection laws in relation to businesses in Pakistan? How would these laws affect cross-border data flows and the daily business of these companies? What are the ways through which Pakistani businesses can adjust appropriately to cope with compliance? To realize these aims, the current research examines the scope

of influence of foreign data protection regulations on Pakistani enterprises and the legal challenges that confront this group and how they can be addressed to ensure more of them comply and remain as resilient as possible (Men et al., 2023).

This is a qualitative and literature-based study that relates to case studies and case laws undertaken to plot laws on data protection across different jurisdictions. This study discusses the issues and opportunities presented to Pakistani businesses by foreign data protection laws and synthesizes different sources. Moreover, the practical perspective of the way these laws are applied could also be introduced by interviewing industry professionals and lawyers (Malgieri, 2023).

Section 2 provides the research methodology. Section 3 offers a literature review concerning extraterritoriality in data protection laws. Section 4 evaluates the mechanism of the "effects doctrine" and developments in the US. Specific compliance burdens for Pakistani SMEs are discussed in Section 5 , while Section 6 evaluates strategic legal solutions for cross-border data transfers. Section 7 examines the status of existing data protection laws in Pakistan and compares them with international standards. Strategic suggestions for enhancing compliance and streamlining operations are discussed in Section 8. The concluding Section 9 summarizes the findings and recommends future research areas (Marques & Alvim, 2021).

Research Methodology

This study adopts a qualitative and literature-based approach to examine the legal issues that Pakistani SMEs encounter with respect to global data privacy. This study applies a doctrinal methodology to examine the main regulations, such as the EU GDPR and the California CCPA, and contrasts them with the legal frameworks that exist in Pakistan, such as PECA 2016 and the draft PDPB 2023. This study uses case studies of successful Pakistani businesses to contribute to the practical depth and synthesize the findings of industry professionals to determine effective compliance strategies. This multidimensional analysis shows that the findings are not only theoretically justifiable but also practically applicable by legal practitioners and business leaders.

Understanding the Extra-Territorial Reach of Foreign Data Protection Laws

In the digital economy, where extraterritoriality in data protection laws has become topical, recent regulations, such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are concerning. These laws capture the intricacies and difficulties in extending national laws beyond borders in the context of an increasing trend among jurisdictions to exercise extraterritorial control over the processing of data from their residents, even where processing took place outside those jurisdictions. As an example, the GDPR applies to companies not domiciled in the EU that process personal data of EU residents to oblige companies outside the EU, such as those in the U.S. and some Latin American countries such as Brazil and Mexico, to comply (Kuner, 2019).

This extraterritoriality is a subset of a wider trend in which jurisdictions take advantage of their substantial market strength to impose their data protection norms on the rest of the world, commonly known as the "California Effect" (Harding et al., 2019). The extensive scope of the GDPR is intended to harmonize data protection laws across the EU and ensure the equal protection of people's privacy. Nevertheless, these extraterritorial claims raise critical questions regarding their legitimacy and enforceability (Chukwurah, 2024). The application of the same laws, especially in cyberspace, is based not only on direct legal instruments but also on indirect ones, which include reputational risk and international collaboration. These laws are not reciprocal and may cause a clash with other jurisdictions, as illustrated in the EU and US approaches, and the likelihood of other leading economies also going in the direction of extraterritorial actions, as in Ehimuan et al. (2024). Moreover, the global jurisdiction is enhanced by technological improvements, including cloud computing and the set of features associated with it, which necessitates a clear grasp of the principles of international law to know whether the extraterritorial extension of jurisdiction is allowed (Aldoseri & Al Khalifa, 2023).

Artificial Intelligence (AI) and machine learning technologies have rapidly taken the global digital economy by storm, further complicating the extraterritorial reach of data protection laws. Cross-border data transfers have grown in volume and complexity as more and more enterprises have adopted cloud-based artificial intelligence (AI) services, generative models,

and predictive analytics, which are mostly located in different jurisdictions, such as the United States and the European Union (Aldoseri & Al-Khalifa, 2023). If you're a small business in a country that's still in the process of rolling out legislation, like Pakistan, you'll need to allow these foreign tools to access local consumer data, which will then be stored on servers under the control of other strict data protection laws like GDPR and CCPA. This can lead to complex compliance implications around data minimization and automated decision making and heighten inadvertent compliance risks. As a result, the combination of AI implementation and extraterritorial data privacy is a key modern frontier, pushing SMEs to deal with competing territorial requirements and endeavoring to capitalize on cutting-edge computational resources to stay competitive globally (Okoli et al., 2024).

The Mechanism of the "Effects Doctrine" and Universal Jurisdiction

The extension of data protection laws across physical boundaries is supported by the effects doctrine, in which a state asserts its jurisdiction because a given activity, despite placing it in another state, produces a significant impact within its jurisdiction. This is enshrined in Article 3(2) of the GDPR, which expands the scope of the regulation to controllers or processors not incorporated in the Union in which the processing activities are connected to the provision of goods or services to the data subjects in the Union or to the surveillance of their actions (Oyeniran et al., 2024). This change is a transition of territorial sovereignty to a subject-based jurisdictional model.

Businesses must straddle this thin thread because they are also considered in terms of the operational implications of these extraterritorial data protection laws (Ngesa, 2024). Considering that the GDPR is extraterritorial, firms operating on a global scale will have to renegotiate their data processing practices and, in the vast majority of cases, spend substantial amounts of money on compliance systems to avoid massive fines and losses of reputation (Okoli et al., 2024). The GDPR has not only passed the test in Europe but has also set a golden standard for offering data protection globally. Kuner (2019) claims that numerous nations have signed similar values to make sure that they are consigned to their standards because consistency towards more aggressive data privacy norms has been witnessed.

The enforcement of the extraterritorial provisions of the GDPR is,

however, problematic in that jurisdictions without reciprocal legal frameworks or treaties with the EU are affected. For example, the enforcement of EU sanctions in countries such as Indonesia or Pakistan is unlikely without local consent or international judicial assistance (Dhar, 2021). Nevertheless, the GDPR's extraterritorial reach is thought to promote trust in data protection, albeit at the cost of respect for other rights, including freedom of expression (Millagala, 2023).

The California Consumer Privacy Act (CCPA) and US Developments

The California Consumer Privacy Act (CCPA) took effect in January 1, 2020 and marked a major move in the U.S. data privacy law by bringing the extraterritorial reach akin to the GDPR. This means that the CCPA applies to businesses outside California that collect personal data from residents of California so long as the business meets specific thresholds regarding revenue or the volume of personal data they process (Hindle, 2020). This extraterritorial application follows broader trends in the extraterritorial application of data privacy laws globally, as other jurisdictions also expand their jurisdiction over data processing activities concerning their residents, even if undertaken outside those jurisdictions (Kretschmer et al. 2021).

Table 1

A Comparative Analysis of the GDPR and CCPA Regulatory Frameworks

Regulatory Aspect	GDPR (European Union)	CCPA (California, USA)
Enforcement Date	May 25, 2018	January 1, 2020
Jurisdictional Basis	Target-subject location (Article 3)	Target-consumer location & Revenue
Key Thresholds	Any processing of EU resident data	$25M revenue or 50k+ records
Primary Penalty	4% of global turnover or €20M	$7,500 per intentional violation
Core Principle	Privacy by Design & Accountability	Transparency & Consumer Control

Discussion has arisen regarding where the CCPA would have extraterritorial scope and whether it could run afoul of the Dormant Commerce Clause; some have argued, however, that the CCPA should be exempt from such challenges in light of its prominence as consumer privacy

protection (Tran, 2024). The rapidly evolving field of data protection regulations has resulted in the CCPA being amended multiple times to increase consumer rights and impose additional data privacy compliance requirements upon businesses, which includes the recent California Privacy Rights Act (CPRA). Driven by these developments, corporations are obligated to stay alert and ready to change in compliance with regulatory changes, as noncompliance subjects them to harsh penalties such as legal actions and the loss of consumer trust.

Data privacy laws with extraterritorial reach are continuing to evolve, and these laws, along with examples such as the GDPR, demonstrate their relevance to the emerging world of cross-border data protection in a more networked world. These laws extend beyond attaining compliance but require a paradigm shift in the manner in which businesses conduct data governance, risk management, and consumer confidence. On the one hand, organizations should fulfill their legal expectations; on the other hand, they should be actively involved in the ethical discourse on the topic of data protection and ensure that they do not breach the rights of the population, as well as the potential of innovations and economic development. Regulators in jurisdictions worldwide are starting to assert their regulatory power in data processing operations, which may potentially impact the people who live in their jurisdiction, leaving organizations with a shifting legal environment, both international law principles and effective data protection practices, within which the organization must act.

Compliance Burdens and Challenges Faced by Pakistani SMEs

The small- and medium-sized enterprise landscape in Pakistan is vibrant and entrepreneurial, with a high degree of vibrancy added to Pakistan's economic fabric. SMEs are important to the generation of employment and the creation of economic growth, and their share of the total workforce and industrial output is large in Pakistan, as per data from the Pakistan Bureau of Statistics. However, when attempting to reach markets abroad, these businesses become entangled in an increasingly complex web of international data protection regulations. This part further intensifies these compliance burdens and challenges for Pakistani SMEs and explores the variety of regulations that they have to address within these complex regulatory environments.

The data protection regulations are numerous, and most of them are not

similar, which is one of the main concerns that Pakistani SMEs have. The resource flow of larger corporations can place people in determined legal units, and SMEs usually possess very limited personnel and money. For example, laws such as the GDPR and the CCPA play a significant role in ensuring that consumers are not exploited; however, they can be cumbersome, particularly for small businesses (Gorondutse et al., 2021). These rules are not an aspect of the theory of SMEs that are involved in doing e-commerce business with European clients or conducting business in California, but practical operational matters that require urgent attention. Employing legal professionals to translate these regulations may be costly, and as such, it is financially inaccessible and may consume the essence of business finances (Asgary et al., 2020).

Technical Obstacles and Data Mapping Complexities

There is also a huge number of SMEs that lack the managerial and technical skills to follow the same rules simply because the users are not educated about data protection practices, and internal processes must be reconfigured (Thomas et al. 2022). There is another monumental challenge to the practical application of data protection measures in data mapping. This can be especially problematic for SMEs that have accrued their digital infrastructure in a haphazard manner over time, as it is easy to understand what data are stored where and how they can be processed. Data are usually stored locally on all sorts of platforms and other cloud services without adequate documentation and monitoring (Zamani, 2022).

Most SMEs are too expensive to invest in the technology and human resources needed to implement an effective records management system to track data processing activities and consent mechanisms (Hou et al., 2020). Moreover, the high cost of secure data (encryption and access control) makes the cost of doing business high, and thus may be extremely expensive for small businesses. The notion of a data protection impact assessment (DPIA) and the principle of privacy by design demand some degree of legal and technical know-how, which is not always present in Pakistani SMEs.

Administrative Capacity and Legal Friction

The administrative capacity needed for understanding the nuances of data subject rights—access, rectification, erasure and data portability—is simply beyond the scope of many SMEs (Al-Mutawa & Al Mubarak, 2024). Establishing processes to manage and respond to data subject requests

within the required timelines can be particularly burdensome, further complicating compliance efforts Mausa and Safina (2024). The compliance burden that Pakistani SMEs face is compounded by the subject of navigating the ambiguous and sometimes contradictory requirements across multiple jurisdictions.

Table 2

Data Protection Compliance Factors: Large Corporations vs. Pakistani SMEs

Compliance Factor	Large Corporations	Pakistani SMEs
Legal Personnel	Dedicated in-house counsel	External/Limited expertise
Budget	Multi-million dollar allocation	Constraint-driven spending
Infrastructure	Centralized Data Warehouses	Organic/Fragmented cloud use
Regulatory Knowledge	Specialist compliance teams	Generalist management
Response Speed	Fast (automated portals)	Slow (manual processes)

The principle of data localization, which requires that data about citizens be stored within geographical limits, presents formidable logistical and financial hurdles to SMEs operating in the global marketplace (Ogbeide et al., 2023). Alternatively, setting up data storage infrastructure across jurisdictions could be financially unviable, and interpreting data transfer restrictions is complex, requiring legal know-how that would be out of the reach of most SMEs (Njilu, 2023). The process of notifying breaches becomes messy due to multiple jurisdictions with their respective procedural requirements and timelines (Nyamwesa, 2024).

However, Pakistani SMEs have strategies to counter these challenges to reduce the compliance burden. Priority is given to the risk management of data processing activities that pose the highest risk to individuals (Rehman et al., 2023). Leveraging cost-effective technologies, such as cloud-based privacy management tools, can streamline data mapping and consent management processes without necessitating significant upfront investments Kisavi and Rotich (2023). Additionally, fostering a culture of privacy inside an organization among employees and offering easily

available training materials reduces compliance risks (Abdul & Goyayi, 2023). Other important tools are data transfer requirement legal strategies. Although Pakistan does not have an adequacy decision from the EU at this time, SMEs might aim at a longer goal to have stronger domestic data protection laws (Nuryyev et al., 2020).

Legal Strategies for Navigating Conflicting Obligations and Cross-border Data Transfers

Data flows are unprecedented in the modern digital economy but present a complicated array of legal challenges to businesses that work internationally. Given the many conflicting data protection obligations between and among such regimes, this web is not easy to navigate for Pakistani enterprises. When personal data from Pakistan are transferred to a cloud server in the European Union or when data from some Californian customers are processed, the GDPR or CCPA are applied (Younas & Mirzaraimov, 2021). In keeping with these potentially conflicting legal mandates and the necessity of their compliance, this part examines some of the existing legal strategies of Pakistani businesses as they attempt to overcome the legal hurdles of lawful transfers of data across borders.

Standard Contractual Clauses (SCCs) and Transfer Impact Assessments (TIAs)

Standard contractual clauses (SCCs) are among the most widespread mechanisms for legitimate cross-border data transfer. The European Commission provides these preapproved sets of contractual terms to ensure that when the data are being transferred from one country to the other, they receive protection equivalent to that provided in the original jurisdiction (Krimmer et al., 2021). For Pakistani businesses that interact with data importers in the EU, SCCs must function at least as an interface to demonstrate that such businesses are complying with the GDPR's part V.

Table 3

Application of EU Standard Contractual Clauses (SCCs) Modules in the Pakistani B2B Context

SCC Module	Exporter Role	Importer Role	Application in Pakistan
Module	Controller	Controller	Direct B2B transfers

SCC Module	Exporter Role	Importer Role	Application in Pakistan
Module 2	Controller	Processor	Outsourcing to Pakistani IT
Module 3	Processor	Processor	Sub-processing in Pakistan
Module 4	Processor	Controller	Processing EU data in Pakistan

In practice, however, the insertion of the clauses alone does not suffice. Pakistani businesses are also obligated to conduct a 'transfer impact assessment' to ascertain whether the laws and practices of the recipient country ensure an adequate level of protection for the data, despite the contractual safeguards offered by the SCCs (Article 46, GDPR). This requires a nuanced understanding of the legal landscape of the recipient country, which can be especially difficult for SMEs to achieve, as they lack in-house legal expertise (Qamar et al., 2021).

Binding Corporate Rules (BCRs) and Privacy Policies

Another mechanism available for legitimizing data transfers is Binding Corporate Rules (BCRs). The application of BCRs for Pakistani SMEs is, however, much more limited. Unlike SCCs, BCRs are internal codes of conduct for data protection that multinational groups of companies must follow when transferring personal data from their employees and customers outside the European Economic Area (EEA) (Kununka et al., 2018). The approval of BCRs is a rigorous and resource-intensive process involving the documentation of every data processing activity, along with internal governance structures.

Privacy policies are foundational legal documents that establish how an organization processes data and outline the commitment to data protection principles. A privacy policy for Pakistani businesses operating abroad must cover the transfer of data to third countries, indicate the legal ground for such transfer (for example, by relying on SCCs) and contain information about risks. Transparency is crucial, but data protection laws cannot be superseded by a privacy policy, and the outcome of an unlawful transfer of data remains invalid even if mentioned in a policy. The success of the policy depends upon its clarity, its accessibility and the fact that real data processing practices of the organization correspond with the statements

made in the policy (Younas & Mirzaraimov, 2021).

Data Protection Impact Assessments (DPIAs) and Schrems II

In particular, the Schrems II decision made Data Protection Impact Assessments (DPIAs) quite prominent concerning cross-border data transfers. Originally, DPIAs were designed as instruments to assess the dangers of precise data handling exercises, yet at present, they include a detailed examination of the legal conditions of the beneficiary country to check whether SCC contractual safeguards are effective (Igbinenikaro & Adewusi, 2024). The DPIA is a critical exercise for Pakistani businesses, which must use SCCs to transfer data to countries that may have intrusive government surveillance laws. It may also require an analysis of the law of the country in which the receiver is located and additional measures such as encryption or pseudonymization to ensure that the data are protected.

The Schrems II decision of the Court of Justice of the European Union decisively changed the world of international data transfers. It revoked the EU-US Privacy Shield framework and put more emphasis on businesses, based on which SCCs were used to rigorously evaluate the legal framework in the recipient country. This is a tremendous challenge for Pakistani businesses because legal guarantees do not just take place by the mere establishment and implementation of SCCs within specific jurisdictions. They are now more closely examined regarding the legal regulations of the recipient country, and in some instances, other measures aimed at possible threats are implemented. The pressure is unevenly distributed on the shoulders of SMEs that have fewer resources and experience (Staunton et al., 2025).

Specific Challenges and the Developing Pakistani Framework

This has exposed SMEs to legal confusion in Pakistan, especially when dealing with international standards, due to the lack of a broad national law on data protection. Although Article 14(1) of the Constitution of Pakistan provides a constitutional safeguard in terms of the right to privacy, the absence of a comprehensive legislative framework has led to an ad hoc strategy based on industry-specific laws (Halim et al., 2022; Masudi & Mustafa, 2023).

Transition to the Personal Data Protection Bill (PDPB) 2023

The Pakistani government recently proposed the Personal Data

Protection Bill (PDPB) 2023, the main goal of which is to increase the level of data protection in accordance with international norms, which requires such critical provisions as regulations concerning data processing, transparent definition of personal data, and the creation of the National Commission of Personal Data Protection (NCPDP) by which compliance can be controlled, which, in turn, has caused certain concerns regarding the possible overextension of the state.

Table 4

Comparative Overview of Pakistan's Data Protection Legislation (PECA 2016 and Draft PDPB 2023) against the GDPR

Feature	PECA 2016	PDPB 2023 (Draft)	GDPR Comparison
Primary Focus	Cybercrime/Telecommunications	General Data Privacy	General Data Privacy
Governance	Federal Investigation Agency	National Commission (NCPDP)	Data Protection Authorities
Subject Rights	Minimal/Implicit	Access, Correction, Erasure	Access, Portability, Erasure
Data Transfers	No general provisions	Localization requirements	Adequacy/SCCs/BCRs
Status	Active Legislation	Under deliberation	Active Legislation

Before the changes in the legislation of data privacy in Pakistan, the nation had been using the Prevention of Electronic Crimes Act (PECA), which covers some areas of cybersecurity but does not have a consistent system to safeguard the personal data of all industries and leaves individuals susceptible to unauthorized data utilization and violation.

Jurisdictional Conflicts and Enforcement Gap

The contradiction between international requirements and local regulations regarding adequacy, local surveillance, and data retention is one of the most topical issues. According to the GDPR, the European Commission evaluates the level of protection afforded by a third country as adequate. The existing legal system in Pakistan, which is typified by the state surveillance authority under PECA, frequently does not pass these tests of adequacy, and businesses must therefore turn to more detailed

processes, such as SCCs with technical back-ups.

The fact that the population is not informed about their rights and responsibilities in relation to data privacy implies that it is more challenging to implement rules concerning data protection efficiently (Masudi & Mustafa, 2023). In most newly established nations, it is challenging to establish good data privacy policies because of institutional incapacity, technical knowledge, and knowledge of the people. A comparative analysis suggests that data protection by incremental reform, together with capacity building specific to each aspect, could bridge the gap between developing and developed nations (Halim et al., 2022).

Strategic Suggestions for Compliance and Operational Resilience

By studying the experience of other SMEs in Pakistan, Pakistani SMEs can reduce the burden of compliance and enhance their operational resilience. According to case studies, compliance does not require huge investments; it can be performed strategically and step-by-step with the help of clear policies, procedures, and educated personnel (Herce et al., 2024).

Developing a Culture of Compliance

Emphasis should be placed on establishing a culture of privacy within the organization. It involves both technical solutions and complete transformation in data processing by all staff members. Accidental data breaches are mostly related to human error rather than technical failure, and specific training and access to resources can reduce the prevalence of these accidents (Abdul & Goyayi, 2023). Government and industrial associations can help and advice SMEs to build proper data protection.

Technical and Tactical Recommendations

- *Risk-Based Prioritization:* SMEs should focus their compliance efforts on data processing activities that pose the highest risk to individuals' rights (Rehman et al., 2023).
- *Adoption of Privacy Tech:* Leveraging cloud-based privacy management tools can automate data mapping and consent management processes, making them more manageable for small teams.
- *Implementation of SCCs with Supplemental Measures:* For cross-border transfers, businesses must use SCCs but should add technical safeguards like end-to-end encryption to address potential legal gaps in the

recipient country (Dorner et al., 2024).

- *National Framework Advocacy:* SMEs should work through industry associations to advocate for a complete national data protection framework that meets international standards while considering the specific challenges faced by small businesses.

One of the most noticeable steps in this direction is the creation of an independent data protection authority and the revision of laws to align with international standards to attract global investment, facilitate the operation of digital businesses, and create confidence in the Pakistani digital economy (Hussain, 2023). The creation of data protection institutions and the improvement of laws with international standards would contribute to the reduction of conflicts arising from conflicting legal requirements.

Conclusion and Future Research

Pakistan small and medium-sized enterprises must find their way in a more digitally connected world with many foreign data protection regimes with unique and often incompatible demands. This discussion has revealed that these regulations impose major compliance costs, such as legal advisory and operational changes, in addition to sound data security provisions. In addition, the discussion of the legal practices that are already in place to facilitate the cross-border transfer of data, including Standard Contractual Clauses and Data Transfer Impact Assessments, reveals the vulnerability of the practices in the face of discussing the right application of data protection.

Overall, empowering and engaging Pakistani SMEs in the international market requires complex solutions, both in the form of streamlined compliance procedures and available support and the further evolution of the national data protection system. The solution to these issues is not only connected to adherence to the law but also to a vital route to promote economic development and innovation in a vibrant SMEs environment in Pakistan. The findings of this study give rise to several suggestions. First, it is necessary to introduce a comprehensive system of national data protection according to international standards, which considers the peculiarities of SMEs. Second, we can contribute to raising awareness and knowledge about data protection laws to make them more compliant through the impartation of specific training and resources. Lastly, the establishment of international collaboration through dialog to establish data

protection standards may ease conflicts of jurisdiction. As countries collaborate to establish balanced data protection systems, cross-border data flows have become easier and more supportive of the global competitiveness.

Further work ought to be on the quantitative effect of compliance costs on the profitability of Pakistani-based IT-enabled service providers, besides investigating the possibilities of utilizing blockchain-based solutions to automate the compliance cost of privacy across borders. With the digital world continually undergoing transformation with AI and big data, the nexus of technological innovation and privacy rights will continue to be a key area of concern for both business leaders and legal experts. In summary, data protection is a dynamic border, and the maze would be tricky, but strategic intervention and policy changes would provide a certain way of operational stability and global prosperity for Pakistani companies.

Author Contribution

Syed Suliman Ali: Conceptualization, methodology, formal analysis, writing – original draft. **Nazli Ismail Nawang:** Supervision, validation, writing - review & editing. **Mohd Badrol Bin Awang:** writing – original draft, writing - review & editing, formal analysis.

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

No datasets were generated or analyzed; this is doctrinal legal research.

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

Abdelkarim, Y. A. (2024). A multi-dimensional approach to impose universal jurisdiction in international legal practice. *International Journal of Law in Changing World*, *3*(1), 21–52. https://doi.org/10.54934/ijlcw.v3i1.87

Abdul, A., & Goyayi, M. L. J. (2023). Potential risks of cloud computing in financial institutions in Tanzania: Perspectives from CRDB Bank Plc. *European Journal of Theoretical and Applied Sciences*, *1*(6), 43–53.

https://doi.org/10.59324/ejtas.2023.1(6).05

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: Concepts, opportunities, and challenges. *Applied Sciences*, *13*(12), Article e7082. https://doi.org/10.3390/app13127082

Al-Mutawa, B., & Al Mubarak, M. M. S. (2024). Impact of cloud computing as a digital technology on SMEs sustainability. *Competitiveness Review: An International Business Journal*, *34*(1), 72–91. https://doi.org/10.1108/CR-09-2022-0142

Asgary, A., Özdemir, A. İ., & Özyürek, H. (2020). Small and medium enterprises and global risks: Evidence from manufacturing SMEs in Turkey. *International Journal of Disaster Risk Science*, *11*(1), 59–73. https://doi.org/10.1007/s13753-020-00247-0

Chukwurah, E. G. (2024). Agile privacy in practice: Integrating CCPA and GDPR within agile frameworks in the U.S. tech scene. *International Journal of Scientific Research Updates*, *7*(2), 24–36. https://doi.org/10.53430/ijsru.2024.7.2.0035

Dhar, T. (2021). The California Consumer Privacy Act: The ethos, similarities and differences vis-à-vis the General Data Protection Regulation and the road ahead in light of California Privacy Rights Act. *Journal of Data Protection & Privacy*, *4*(2), 170–192. https://doi.org/10.69554/GLSA8501

Dorner, M., Capraro, M., Treidler, O., Kunz, T.-E., Šmite, D., Zabardast, E., Méndez, D., & Wnuk, K. (2024). Taxing collaborative software engineering: The challenges for tax compliance in software engineering. *IEEE Software*, *41*(4), 143–150. https://doi.org/10.1109/MS.2023.3346646

Ehimuan, B., Obi, O. C., Akagha, O. V., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

Gorondutse, A. H., Arshad, D., & Alshuaibi, A. S. A. (2021). Driving sustainability in SMEs' performance: The effect of strategic flexibility. *Journal of Strategy and Management*, *14*(1), 64–81.

https://doi.org/10.1108/JSMA-03-2020-0064

Halim, W., Upadhyay, A., & Coflan, C. (2022). *Data access and protection laws in Pakistan: A technical review*. EdTech Hub. https://doi.org/10.53832/edtechhub.0098

Harding, E. L., Vanto, J. J., Clark, R., Ji, L. H., & Ainsworth, S. C. (2019). Understanding the scope and impact of the California Consumer Privacy Act of 2018. *Journal of Data Protection & Privacy*, *2*(3), 234–253. https://doi.org/10.69554/TCFN5165

Herce, C., Martini, C., Toro, C., Biele, E., & Salvio, M. (2024). Energy efficiency policies for small and medium-sized enterprises: A review. *Sustainability*, *16*(3), Article e1023. https://doi.org/10.3390/su16031023

Hindle, A. (2020). *Impact of GDPR on identity and access management*. IDPro Body of Knowledge,. https://doi.org/10.55621/idpro.24

Hou, X., Wang, B., & Gao, Y. (2020). Stakeholder protection, public trust, and corporate social responsibility: Evidence from listed SMEs in China. *Sustainability*, *12*(15), Article e6085. https://doi.org/10.3390/su12156085

Igbinenikaro, E., & Adewusi, A. O. (2024). Developing international policy guidelines for managing cross-border insolvencies in the digital economy. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1034–1048. https://doi.org/10.51594/ijmer.v6i4.983

Junejo, I., Kazi, S., Siddiqui, M. B., Ramish, M. S., & Malokani, D. K. A. K. (2023). Impact of legal framework and SCM policies on supply chain collaboration: Role of information technology. *Russian Law Journal*, *11*(10S), 76–84. https://doi.org/10.52783/rlj.v11i10s.1653

Kisavi, S. M., & Rotich, A. (2023). Effect of corporate social responsibility on the financial performance of small and medium enterprises in Makueni Sub-County. *Journal of Finance and Accounting*, *7*(11), 139–161. https://doi.org/10.53819/81018102t5294

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web*, *15*(4), 1–42. https://doi.org/10.1145/3466722

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A.-A. (2021). Developing

cross-border e-governance: Exploring interoperability and cross-border integration. In R. Krimmer & M. R. Johannessen (Eds.), *Electronic participation* (Lecture Notes in Computer Science, Vol. 12849, pp. 107–124). Springer. https://doi.org/10.1007/978-3-030-82824-0_9

Kuner, C. (2019). The internet and the global reach of EU law. In M. Cremona & J. Scott (Eds.), *EU law beyond EU borders: The extraterritorial reach of EU law* (pp. 112–145). Oxford University Press. https://doi.org/10.1093/oso/9780198842170.003.0004

Kununka, S., Mehandjiev, N., & Sampaio, P. (2018). A comparative study of Android and iOS mobile applications' data handling practices versus compliance to privacy policy. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), *Privacy and identity management. The smart revolution* (IFIP Advances in Information and Communication Technology, Vol. 526, pp. 301–313). Springer. https://doi.org/10.1007/978-3-319-92925-5_20

Malgieri, G. (2023). In/acceptable marketing and consumers' privacy expectations: Four tests from EU data protection law. *Journal of Consumer Marketing*, *40*(2), 209–223. https://doi.org/10.1108/JCM-03-2021-4571

Marques, A. L., & Alvim, A. T. B. (2021). Construction of sustainable territories and the multiple dimensions of sustainability: An assessment of urban and environmental instruments in the Juqueri-Cantareira Sub-basin of the São Paulo Metropolitan Region. *Frontiers in Sustainable Cities*, *3*, Article e670985. https://doi.org/10.3389/frsc.2021.670985

Masudi, J. A., & Mustafa, N. (2023). Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age. *Pakistan Journal of International Affairs, 6*(3), 356–366. https://doi.org/10.52337/pjia.v6i3.906

Mausa, O. H., & Safina, M. (2024). Perceptions of tax compliance willingness among SME owners in KCCA, Uganda. *International Journal for Multidisciplinary Research*, *6*(4), 1–8. https://doi.org/10.36948/ijfmr.2024.v06i04.23334

Men, F., Yaqub, R. M. S., Yan, R., Irfan, M., & Haider, A. (2023). The impact of top management support, perceived justice, supplier management, and sustainable supply chain management on moderating

the role of supply chain agility. *Frontiers in Environmental Science*, *10*, Article e1006029. https://doi.org/10.3389/fenvs.2022.1006029

Millagala, K. (2023). Navigating the confluence of artificial intelligence and social media marketing. *International Journal of Research Publications*, *133*(1), 19–35. https://doi.org/10.47119/IJRP1001331920235473

Ngesa, J. (2024). Tackling security and privacy challenges in the realm of big data analytics. *World Journal of Advanced Research and Reviews*, *21*(2), 552–576. https://doi.org/10.30574/wjarr.2024.21.2.0429

Njilu, M. (2023). Tax compliance among small and medium manufacturing enterprises in Kenya: Does tax morale matter? *Rowter Journal*, *2*(1), 46–55. https://doi.org/10.33258/rowter.v2i1.836

Nuryyev, G., Wang, Y.-P., Achyldurdyyeva, J., Jaw, B.-S., Yeh, Y.-S., Lin, H.-T., & Wu, L.-F. (2020). Blockchain technology adoption behavior and sustainability of the business in tourism and hospitality SMEs: An empirical study. *Sustainability*, *12*(3), Article e1256. https://doi.org/10.3390/su12031256

Nyamwesa, A. (2024). Cloud computing technology adoption: Challenges for SMEs, a case of selected SMEs in Tanzania. *International Journal of Advanced Business Studies*, *3*(2), 1–12. https://doi.org/10.59857/IJABS.3118

Ogbeide, V. O., Omorogiuwa, O., & Salami, E. E. (2023). An empirical survey to substantiate the need for a cyber security framework for SMEs in Nigeria. *International Journal of Research Publications*, *128*(1), 281–296. https://doi.org/10.47119/IJRP1001281720235221

Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286–2295. https://doi.org/10.30574/wjarr.2024.21.1.0315

Oyeniran, O. C., Modupe, O. T., Otitoola, A. A., Abiona, O. O., Adewusi, A. O., & Oladapo, O. J. (2024). A comprehensive review of leveraging cloud-native technologies for scalability and resilience in software development. *International Journal of Science and Research Archive*, *11*(2), 330–337. https://doi.org/10.30574/ijsra.2024.11.2.0432

Qamar, A., Javed, T., & Beg, M. O. (2021). *Detecting compliance of privacy policies with data protection laws*. ArXiv Preprint. https://arxiv.org/abs/2102.12362

Rehman, S. U., Al-Shaikh, M., Washington, P. B., Lee, E., Song, Z., Abu-AlSondos, I. A., Shehadeh, M., & Allahham, M. (2023). Fintech adoption in SMEs and bank credit supplies: A study on manufacturing SMEs. *Economies*, *11*(8), Article 213. https://doi.org/10.3390/economies11080213

Santema, P., & Kempenaers, B. (2023). Patterns of extra-territorial nest-box visits in a songbird suggest a role in extra-pair mating. *Behavioral Ecology*, *34*(1), 150–159. https://doi.org/10.1093/beheco/arac111

Staunton, C., Edgcumbe, A., Abdulrauf, L., Gooden, A., Ogendi, P., & Thaldar, D. (2025). Cross-border data sharing for research in Africa: An analysis of the data protection and research ethics requirements in 12 jurisdictions. *Journal of Law and the Biosciences*, *12*(1), Article elsaf002. https://doi.org/10.1093/jlb/lsaf002

Thomas, A., Scandurra, G., & Carfora, A. (2022). Adoption of green innovations by SMEs: An investigation about the influence of stakeholders. *European Journal of Innovation Management*, *25*(6), 44–63. https://doi.org/10.1108/EJIM-07-2020-0292

Younas, A., & Mirzaraimov, B. T. O. (2021). To what extent are consumers harmed in the digital market from the perspective of the GDPR? *International Journal of Multidisciplinary Research and Analysis*, *4*(8), 1187–1192. https://doi.org/10.47191/ijmra/v4-i8-17

Zamani, S. Z. (2022). Small and medium enterprises (SMEs) facing an evolving technological era: A systematic literature review on the adoption of technologies in SMEs. *European Journal of Innovation Management*, *25*(6), 735–757. https://doi.org/10.1108/EJIM-07-2021-0360