SDPI
Sustainable Development Policy Institute

POLICY BRIEF

STRENGTHENING DATA GOVERNANCE IN PAKISTAN FOR INCLUSIVE AND SECURE DIGITAL TRANSFORMATION

AUTHOR: AYESHA NAEEM

A publication of the Sustainable Development Policy Institute (SDPI).

Sustainable Development Policy Institute is an independent, non- profit research institute on sustainable development.

First edition: September 2025 © 2025 by the Sustainable Development Policy Institute

Mailing Address:

PO Box 2342, Islamabad, Pakistan

Telephone: 0092-51-2278134, 2278136, 2277146, 2270674-76

Fax: 0092-51-2278135,

URL: www.sdpi.org

Abstract

Pakistan's rapid digital adoption has made data central to governance, service delivery, and economic growth, yet its governance remains fragmented, inconsistent, and under-regulated. The Digital Nation Act and the Draft Personal Data Protection Bill represent important steps forward but require clearer safeguards, stronger institutional independence, and effective enforcement. This brief outlines the systemic challenges, legal contradictions, lack of interoperability, weak enforcement, and limited transparency. It draws lessons from global practices. The way forward lies in strengthening legal protections, ensuring independent oversight, adopting interoperable open-data standards, and developing secure digital public infrastructure. By doing so, Pakistan can enable inclusive governance, promote innovation, and build citizen trust in its digital future.

Contents

1. Introduction 5
1.1. Background 5
1.2. Scope and Objectives 6
2. Methodology 7
3. Pakistan's Current Data Governance Landscape 7
3.1. Evolving Legal and Policy Framework 7
3.2. Digital Nation Pakistan Act (2025) 8
3.3. Draft Personal Data Protection Bill (2023) 10
3.4. Persistent Systemic Challenges 11
4. Recommendations and Way Forward 17
4.1. Legal and Regulatory Reforms 17
4.2. Data Governance and Standards 18
4.3. Digital Infrastructure and Innovation 19
4.4. Cybersecurity and Trust 20
5. Conclusion 21
6. References 22
Annex 1: The Six Attributes of Data Governance Mapping and Their Indicators 25
Annex B: PTA's Steps on Data Protection & Cybersecurity 27

1. Introduction

1.1. Background

The governance of data has become a decisive factor in Pakistan's ability to achieve sustainable development, safeguard citizen trust, and compete in the global digital economy. Every day, vast amounts of personal, financial, environmental, and administrative data are generated by both public and private entities. This data forms the foundation of critical services, from social safety nets and public health systems to infrastructure planning and disaster management. In today's world, data is not just a by-product of governance, it is a strategic national asset, yet stewardship has not kept pace with its centrality.

Pakistan's digital adoption is accelerating, with more than 116 million internet users (about 46 percent of the population) and over 190 million mobile connections, 74 percent broadband-enabled (Frąckiewicz, 2025). IT exports reached a record US$3.2 billion in 2024 (a 24 percent increase) (Profit by Pakistan Today, 2024). Over 21 million customers now actively use mobile banking apps, supported by more than 64 million branchless banking wallets and 13 million internet banking users (Dilawar, 2025). Meanwhile, the Raast instant payment system has seen explosive growth, with 294 million peer-to-peer transactions worth Rs 6.1 trillion in Q2FY25 alone, a 50 percent increase in volume and a 32 percent increase in value compared to the previous quarter (State Bank of Pakistan, 2025). This scale amplifies both opportunity and exposure: weak governance increases risks of cyberattacks, privacy violations, and economic inefficiencies. Recent breaches, such as the NADRA data leak that compromised the information of 2.7 million citizens and the Bangladesh central bank breach, show how data failures can cascade into financial and security crises (Raza, 2025).

Despite notable policy movement, Pakistan's data governance ecosystem remains fragmented and inconsistent. Privacy is recognized as a constitutional right, yet successive governments since 1973 have not enacted a comprehensive, enforceable data protection law; the 2019 Open Data policy remains unapproved; and the Right to Information regime, elevated to a fundamental right and replicated across federal and provincial statutes, suffers from weak implementation and under-resourced commissions. In practice, Pakistan has relied on reactive transparency while neglecting the development of proactive openness. Effective governance demands both, timely, specific disclosures when requested and systemic, open data that enables research, accountability, and innovation.

Table 1: Pakistan and selected regional and income peer countries' total scores and attributes on Global Data Governance Mapping 2024 (The six attributes of data governance and their 26 indicators are detailed in Annex A)

Country	Overall Score	Strategic	Regulatory	Responsible	Structural	Participatory	International
Pakistan	16	0	20	0	25	33	20
India	28	50	20	20	25	33	20
Nigeria	24	25	20	0	25	33	40
Indonesia	36	50	20	0	75	33	40

Source: (Global Data Governance Mapping, 2024)

The enactment of the Digital Nation Act 2025 and the draft Data Protection Bill 2023 are important milestones in the country's journey toward modernizing its digital governance framework. Yet awareness of these laws remains limited, and their adequacy in addressing emerging challenges, from cyber threats to artificial intelligence governance, requires critical evaluation. The obstacles are less about capacity than about political will, consistent enforcement, and structural fragmentation, compounded by infrastructure gaps that leave Pakistan trailing regional peers on international indices of connectivity and readiness. The policy direction is clear; Pakistan needs actionable, high-quality, and shareable data to enable inclusive governance, economic planning, and evidence-based decision-making. Without a coherent balance between openness, privacy, and security, backed by coordination across the federation and credible enforcement, Pakistan risks forgoing the economic, social, and innovation dividends of its data assets just as its digital economy begins to scale.

1.2. Scope and Objectives

In the backdrop of these opportunities and challenges, this brief critically assesses the country's data governance ecosystem. The scope includes an examination of existing laws and policies, regulatory overlaps, institutional capacity, and the implications of the Digital Nation Act 2025 and the draft Data Protection Bill 2023. The key objectives of this brief are to:

- Analyze Pakistan's evolving data governance framework, identifying policy gaps, regulatory conflicts, and lessons from regional best practices.
- Assess the implications of the Digital Nation Act 2025 and the draft Data Protection Bill 2023 for data protection, cybersecurity, equitable access, and digital innovation.
- Recommend regulatory interventions and institutional reforms to standardize data-sharing mechanisms, strengthen enforcement of data protection laws, and build institutional capacity for secure, responsible, and innovation-friendly data governance.

2. Methodology

This policy brief combines primary consultations, secondary research, and comparative analysis. Primary insights were drawn from the Public–Private Dialogue on Data Governance in Pakistan: Policy Reforms and Opportunities for Digital Transformation, organized by the Sustainable Development Policy Institute (SDPI The dialogue convened policymakers, regulators, private-sector representatives, civil society, and digital rights advocates to deliberate on policy gaps and reform opportunities. The insights from this dialogue form the analysis and recommendations presented in this study. Secondary sources, including academic research, regulatory documents, international benchmarks, and the findings from the Data for Development (D4D) Asia study on data governance in South and Southeast Asia, were used to situate Pakistan's experience in a regional and global context. Comparative analysis further highlighted lessons from countries with more mature governance frameworks, providing relevant insights for Pakistan's evolving landscape.

3. Pakistan's Current Data Governance Landscape

3.1. Evolving Legal and Policy Framework

Pakistan's data governance framework has developed incrementally, from the Electronic Transaction Ordinance (2002), which recognized digital records, to the Digital Nation Act (2025). Although privacy is a constitutionally protected right, Pakistan has yet to enact a comprehensive data protection or privacy law, leaving one of the most critical pillars of data governance missing.

In 2019, the Ministry of IT proposed an Open Data Policy to make an inventory for information that is to be open by default, proactively publish datasets in machine-readable formats, and mandate annual Open Data Reports to guide implementation. The draft sought to improve accountability, enable innovation, and encourage citizen engagement under Article 19-A of the Constitution. Yet, it remains unapproved, leaving Pakistan without a systematic framework for data-sharing across government institutions.

The Right to Information (RTI) law, later elevated to a constitutional right, also suffers from weak implementation and under-resourced commissions, limiting its effectiveness. There is currently no dedicated data protection authority. Enforcement is carried out under PECA 2016, which empowers the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA) to act against unauthorized access and regulate the processing and retention of

data. However, PECA provides no comprehensive data security requirements, with protections limited largely to sector-specific regulations such as in banking and finance. A draft Cybersecurity Law aims to establish uniform standards for securing data, systems, and infrastructure across institutions. At present, cybersecurity efforts are fragmented, with individual departments applying their own measures in the absence of a universal framework.

General	Special	Sector Regulators	Frameworks Initiatives	Policies	Draft Policies / Laws
• Constitution of the Islamic Republic of Pakistan 1973 • Digital Nation Pakistan Act 2025 • Electronic Transactions Ordinance 2002 • Right of Access to Information Act, 2017 • The Elections Act, 2017 • National Database and Registration Authority Ordinance, 2000 • Official Secrets Act 1923 • National Archives Act, 1993 • Surveying and Mapping Act, 2014 • The General Statistics (Re-organization) Act, 2011 • Pakistan Climate Change Act 2017	• Federal Investigation Agency Act, 1974 • National Counter Terrorism Authority Act, 2013 • Prevention of Electronic Crimes Act 2016	• State Bank of Pakistan Act 1956 • Pakistan Telecommunication (Re-organisation) Act 1996 • The Exchange Commission of Pakistan Act, 1997 • Pakistan Electronic Media Regulatory Authority Ordinance 2002 • Public Procurement Regulatory Authority Ordinance, 2002 • The Intellectual Property Organization of Pakistan Act, 2012 • The Pakistan Medical and Dental Council Act, 2022	• Open Data Pakistan (HEC, LUMS, NCCB) / Open Government Partnership • Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021 • Critical Telecom Data and Infrastructure Security Regulations 2020 • Enterprise Technology Governance & Risk Management Framework for Financial Institutions, 2017 • Cyber Security Framework – 2022	• Pakistan IT Policy & Action Plan 2000 • De-Regulation Policy 2003 • Mobile Cellular Policy 2004 • Broadband Policy 2004 • Telecommunications Policy, 2015 • National Cyber Security Policy 2021 • Digital Pakistan Policy 2018 • Cloud First Policy 2022 • Pakistan Vision 2025 • Uraan Pakistan • National Artificial Intelligence Policy 2025	• Personal Data Protection Bill, 2023 • Open Data for the Government of Pakistan 2019

Figure 1: Pakistan's Data Governance framework
Source: (LIRNEasia, 2025)

3.2. Digital Nation Pakistan Act (2025)

Until recently, Pakistan lacked a nationwide framework to organize how public institutions plan, exchange, and use data. The Digital Nation Pakistan Act (DNPA) 2025 introduces a a whole-of-government architecture for digital transformation, built on a National Digital Masterplan, common interoperability standards, and a secure data-exchange layer that allows consent-based, real-time verification at source. Prepared under the World Bank's US$78 million Digital Economy Enhancement Project (DEEP), it aims to move routine public services to mobile channels, reduce paperwork, and enable a data-driven economy across sectors such as agri-tech, fintech, ed-tech, and health-tech (Amin, 2024). A Digital Nation Fund is envisaged to finance these transitions. As shown in figure 2, the Act proposes to create three bodies.

National Digital Commission (NDC): Chaired by the Prime Minister with federal and provincial leadership, it sets the strategic vision and policy framework for Pakistan's digital transformation, ensuring alignment and eliminating redundancies across levels of government.

Pakistan Digital Authority (PDA): Responsible for implementing NDC policies, it coordinates and harmonizes digital initiatives across federal, provincial, and local tiers to drive improved service delivery and economic growth.

Strategic Oversight Committee (SOC): Oversees PDA's performance and provides independent review to the NDC, ensuring alignment of implementation with the national digital master plan.

Figure 2: Institutional Architecture under the Digital Nation Act 2025

3.2.1. Implementing Challenges

- The drafting process did not involve broad consultation with civil society or citizen representatives, despite the Bill's far-reaching implications for rights and the digital economy. Additionally, the governance bodies proposed under the Bill do not include representation from ordinary citizens or civil society. This absence of inclusive participation limits opportunities to incorporate diverse perspectives that could strengthen accountability and trust in the proposed system (Digital Rights Foundation, 2025).
- The proposed authorities under the Act overlap with existing entities such as NITB. Broad definitions of "digital economy" and "emerging technologies" further risk duplicating functions, generating inefficiencies, and blurring accountability lines.
- The implementation relies heavily on reliable internet connectivity, which remains inaccessible to more than half of the population. Reportedly, Pakistan's internet speeds were rated among the lowest 12% of the countries (Dawn, 2024). A centralized digital ID system risks exacerbating exclusion rather than improving access to services.
- Sections 28 and 29 give the Bill overriding power over other laws while barring judicial review of actions taken under it. This effectively removes checks and balances, raising constitutional concerns around due process. The Strategic Oversight Committee, despite being labeled "independent," is chaired by the IT Minister, further limiting its autonomy (Digital Nation Pakistan Act, 2025).
- The NDC's composition, 17 members including the Prime Minister, federal ministers, and all provincial chief ministers, concentrates authority at the highest political levels. This centralization risks politicization, delays in decision-making, and difficulties in reconciling federal and provincial interests. The PDA also lacks true autonomy, as appointments and removals rest with the Prime Minister, undermining independence.

3.3. Draft Personal Data Protection Bill (2023)

The Personal Data Protection Bill (PDPB) 2023 is Pakistan's proposed legal framework for safeguarding personal data. It establishes a National Commission for Personal Data Protection (NCPDP), enshrines principles such as purpose limitation, data minimization, accuracy, and retention controls, and grants individuals the rights to access, rectify, erase, port, and object to processing. It also includes breach notification requirements, stricter handling of sensitive data, and rules for cross-border transfers.

3.3.1. Key Challenges

- Earlier drafts of the Bill required localization of "Critical Personal Data." While the forced localization clause has reportedly been removed after opposition from both international and local stakeholders, the revised draft introduces restrictions on transferring sensitive data, such as financial, religious, and genetic information, outside the country unless the recipient state has an adequate legal regime. However, the Bill allows broad exceptions under ambiguous terms like "national security," "public order," and "national interest." These undefined exceptions risk undermining explicit consent as the foundation for cross-border data transfers and leave room for potential misuse, including unlawful surveillance (Digital Rights Foundation, 2024).
- The proposed NCPDP, tasked with implementing and enforcing the law, may lack genuine autonomy. Its placement under federal government control, combined with provisions granting the government power to issue binding policy directives, approve international cooperation, and retain authority to make rules and regulations, compromises the Commission's independence. Such control risks politicizing the body, limiting its effectiveness as an impartial regulator
- The Bill repeatedly invokes "national interest" as a justification for derogations from data protection obligations, but the term is left undefined. This vagueness grants wide discretion to the Commission and the government, creating uncertainty for stakeholders and potentially enabling arbitrary restrictions on rights. Without clarity, the scope of "national interest" could conflict with privacy protections and weaken the overall framework ("Draft Personal Data Protection Bill," 2023).
- The Bill obliges data controllers to notify both the NCPDP and affected individuals within 72 hours of a breach. However, it provides no clear criteria for what constitutes a valid reason for delaying notification beyond that period. This lack of specificity risks inconsistent application, delays in informing individuals, and reduced accountability, which could ultimately compromise the rights and freedoms of data subjects (Digital Rights Foundation, 2024).

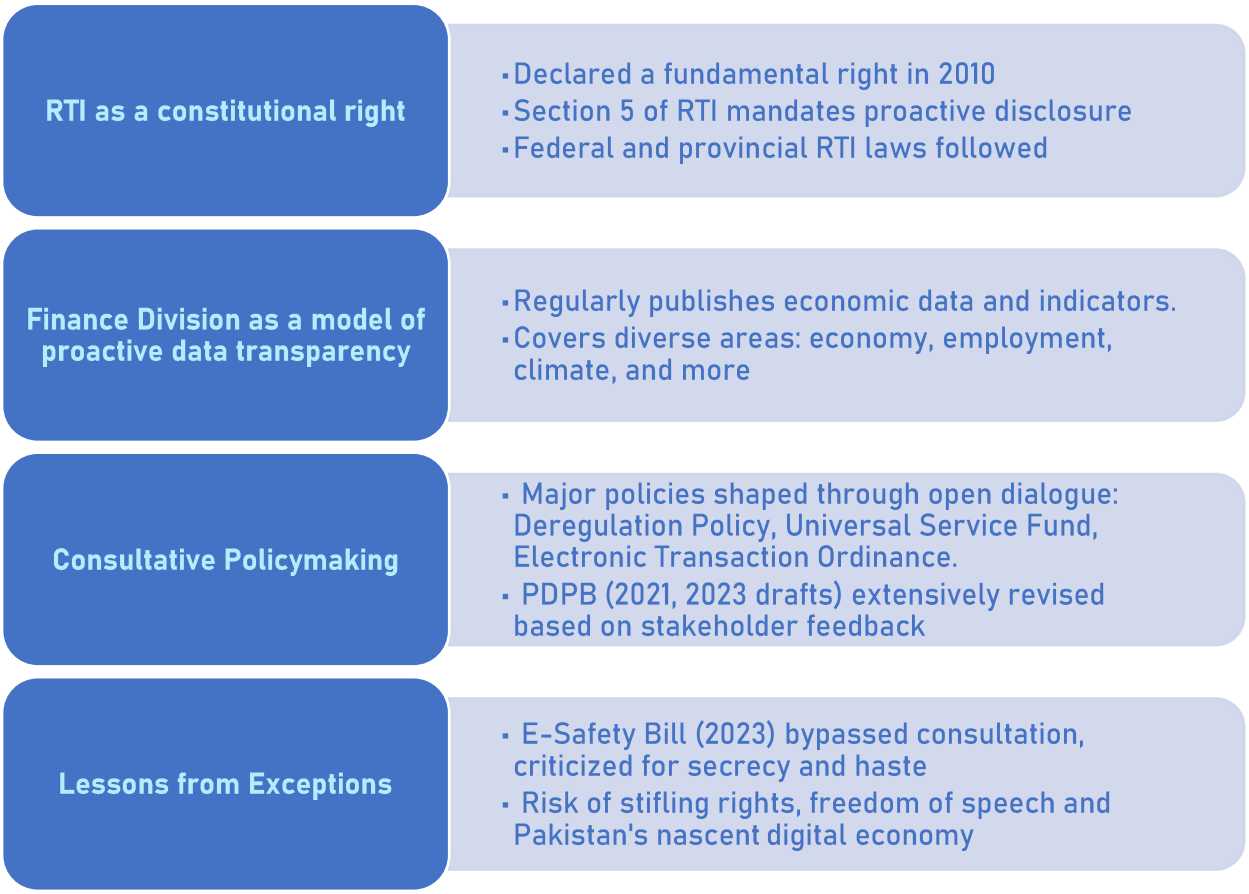

Figure 3: Good Practices in Pakistan's Data Governance Framework

3.4. Persistent Systemic Challenges

3.4.1. Governance & Institutional Framework

- Federal, provincial, and local institutions continue to run isolated databases, often collecting the same type of information without coordination. This duplication not only wastes resources but also leads to duplication, inconsistent recognition of datasets such as BISP/NSER, and mistrust among agencies.
- Data is still stored and disseminated in non-usable formats, such as scanned PDF procurement records or static tables. Without machine-readable datasets, analysis, reuse, and civic or business innovation are blocked.
- The absence of a defined framework for public–private data collaboration, especially in sectors like health and agriculture, means that start-ups and private actors cannot easily build services on top of government datasets. This stifles innovation that could scale public-service delivery.

3.4.2. Legal & Regulatory Framework

- Pakistan's legal landscape is internally contradictory: the Right to Information Act (2017) recognizes citizens' access to information, while the colonial-era Official Secrets Act (1923, amended 2023) criminalizes disclosure in sweeping terms. Officials often default to secrecy, creating a chilling effect even where transparency is lawful.
- The Right of Access to Information Act does not extend to the Supreme Court, which leaves a gap in transparency, as the judiciary's highest body falls outside the Act's scope. By contrast, India and Sri Lanka's RTI laws override secrecy statutes, and in India the Supreme Court has been explicitly subject to RTI, required to record reasons for any denial (Shankar IAS Parliament, 2018) (Supreme Court Observer, 2023).
- The National Archives Act permits disclosure of records after 20 years for research but restricts refusals only on security grounds, not privacy, indicating unclear priorities (National Archives Act, 2016).
- While the Data Protection Bill allows personal data to leave Pakistan with the subject's consent, regulators like PTA and the State Bank prohibit such transfers even with consent. This inconsistency creates legal uncertainty for data controllers and undermines trust in the framework.
- Artificial intelligence requires vast datasets, often including information not provided directly by individuals (e.g., Wikipedia entries). The Personal Data Protection Bill does not address how such data can be used for AI training, creating uncertainty and a gap between emerging AI policy and data protection law.
- Pakistan's National AI Policy was introduced despite the absence of a data protection regime, yet it references provisions of the still-pending Personal Data Protection Bill. This creates legal uncertainty while exposing citizens to heightened privacy risks around large language models. The policy also assigns an AI directorate powers to address disinformation and data breaches, but without clarity on its overlap with the amended Prevention of Electronic Crimes Act (2016) or the proposed Social Media Regulatory Authority (Khilji, 2025). Without parliamentary scrutiny or an inclusive legislative process, such measures risk encroaching on privacy and freedom of expression.

3.4.3. Transparency & Public Access

- Despite Section 5 of the RTI Act mandating proactive disclosure, many agencies publish little or no information, or release it in inaccessible formats. Citizens must rely on litigation or personal networks to access even routine records.
- RTI commissions are underfunded, lack staffing, and struggle to enforce orders, which allows agencies to ignore disclosure obligations without consequence.
- Large infrastructure and surveillance initiatives, such as the rollout of the national firewall, were announced with minimal detail on scope, governance,

or safeguards. This lack of communication promotes speculation and reduces trust in state-led digital projects.

- Pakistan's National AI Policy was drafted without parliamentary debate or transparent multi-stakeholder consultation. Civil society, environmentalists, digital rights experts, media, educators, and healthcare professionals were not included and no clarity exists around the stakeholder engagement process. Significantly, the policy lacks a legislative basis, as no parliamentary debate, including in the IT committees, has taken place, other than the IT ministry formulating the policy through a nontransparent process (Khilji, 2025).

India's Open Access and Data Transparency Initiatives	
CSIR's Open Access Mandate	Open Government Data (OGD) Platform
In India, the Council of Scientific and Industrial Research (CSIR) mandates that all research from its laboratories supported by CSIR grants be made open access through institutional repositories linked by a central harvester. All CSIR journals are progressively moving to open access. CSIR-NISCAIR runs training programs for scientists, editors, and repository staff to build capacity for open access. CSIR scientists are barred from publishing, reviewing, or serving on editorial boards of journals that lack transparent licensing models. Beyond institutional practice, CSIR aims to lead the national Open Access movement by bringing other scientific agencies on board to frame a National Open Access Policy. potentially through legislation, so that all publicly funded research outputs are placed in the public domain ("CSIR Open Access Mandate," 2021).	India has also advanced government data transparency through the Open Government Data (OGD) Platform (data.gov.in) (Saxena, 2012). In compliance with the National Data Sharing and Accessibility Policy (NDSAP), the platform provides single-point, machine-readable, and regularly updated access to datasets, documents, and digital tools from ministries and departments. By releasing government data into the public domain, it promotes transparency, accountability, civic participation, and innovation. India's efforts have gained international recognition, ranking 43 out of 100 on the Open Data Barometer and 33 out of 165 on the Democracy Index (Chakravarty, 2017). The expanding datasets, literature, and applications built on the platform reflect its growing role in promoting open data as a foundation of democratic governance.

South Africa's Green and White Papers

In South Africa, the lawmaking process often begins with a Green Paper, a discussion document prepared by the relevant Ministry or department to outline initial thinking on a policy issue. The Green Paper is published for public comment, allowing citizens and stakeholders to submit suggestions and ideas.

This stage is typically followed by a White Paper, which refines the proposals into a broad statement of government policy. The White Paper is drafted by the department or a task team designated by the Minister, with further input from parliamentary committees. Committees may suggest amendments or alternative approaches, after which the policy is sent back to the Ministry for further discussion and final decisions (The Legislative Process, n.d.).

This two-step process encourages openness, consultation, and iterative refinement before legislation is introduced.

3.4.4. Data Security & Cybersecurity

- NADRA's central database holds the most extensive personal information of citizens, yet bulk sharing with banks, telcos, schools, and provincial programs has extended exposure to systems with weaker security. Once data leaves NADRA, it is often outside effective safeguards.
- Repeated data breaches, such as the Punjab IT Board (PITB) leak in 2018, have exposed citizens' CNICs, scanned ID copies, educational records, and even voter lists, feeding a thriving black market where entire datasets were sold online for as little as Rs. 100. Investigations revealed that the breaches stemmed not from NADRA's core servers directly, but from access extended to PITB for digitization purposes. Despite being written off at times as "technical glitches," these incidents highlight systemic weaknesses: sensitive data is shared widely across departments with minimal safeguards, misuse by insiders goes unchecked, and there are no clear avenues of redress for victims. The persistence of these records years after exposure underscores both the absence of strong data protection legislation and the lack of institutional accountability in breach response and remediation (Attaa, 2018) (Digital Rights Foundation, 2018).
- Compromised biometrics and fraudulent ID issuance have facilitated the creation of gray SIMs. These unregistered or duplicate connections are widely used in scams, financial fraud, and other illicit activity, underlining weak enforcement of verification regimes.
- Cybersecurity regulations for private operators are poorly enforced. Telecoms and app developers often consume sensitive APIs without adopting strong encryption or data-minimization practices. PTA has taken measures through regulations and technical frameworks to secure telecom data and infrastructure (see Annex B for details).
- E-Khidmat centres proposed under the AI Policy, covering services such as health, education, sanitation, energy, and security, envision delivery through AI chatbots, smart reporting, and centralized platforms. While intended to streamline access, these initiatives carry major surveillance risks in the absence of a robust data protection regime. Overreliance on automated

channels also risks replicating the frustrations of existing portals and helplines, where citizens often receive no response when human assistance is needed (Khilji, 2025).

- The National AI policy fails to integrate human rights safeguards, particularly regarding technology-facilitated gender-based violence (TFGBV). AI deepfakes are already being used to target women, showing the disproportionate risks faced by women and gender minorities in the absence of safeguards. While the policy mentions training programmes for women and persons with disabilities, it does not address the expanding role of AI in TFGBV or provide for human rights risk assessments. Without such measures, AI adoption risks creating new harms rather than alleviating existing vulnerabilities.

3.4.5. Standards & Interoperabilit

- Pakistan's digital ecosystem is highly fragmented, with every organization developing its own applications and datasets on different standards. This lack of coordination makes government systems difficult to integrate and prevents efficient use of existing data. At present, there is no comprehensive data standardization policy. Each organization tends to adopt its own data and technology standards, leading to silos that restrict system-wide efficiency, scalability of services, and reuse of existing datasets.
- The absence of a national policy mandating open standards and open-source frameworks has also weakened digital sovereignty and created dependence on a few large IT vendors. Without standardized protocols, public institutions face vendor lock-in, limited flexibility, and higher costs of scaling digital services. This fragmentation extends to accessibility and reporting standards, where global norms (such as ISO, W3C, IETF, and XBRL) are not consistently applied, undermining cross-platform compatibility and usability for both government and citizens.
- There is no government-run data-sharing platform. In contrast, every country covered in the LIRNEasia study, except Pakistan and Nepal, has a government open data portal. Notable examples include Indonesia's One Data Indonesia (Satu Data) and India's NDSAP/data.gov.in, which demonstrate how open data portals can institutionalize transparency, accountability, and innovation.
- Pakistan has no formal program to promote free and open-source software (FOSS), unlike countries such as India, the EU, and the USA, where FOSS adoption is actively encouraged for government systems. The lack of FOSS adoption, combined with the absence of open APIs, has prevented programmatic access to data at scale. Open APIs are crucial for government-to-government, government-to-business, and government-to-citizen data sharing, and their absence has slowed the development of a robust digital public infrastructure
- Legal contradictions, such as those between the RTI Act and the Official Secrets Act, further complicate data access and sharing. NADRA's data-sharing practices, in particular, lack clarity on what constitutes open versus protected data, generating institutional confusion and inconsistent disclosure. Similarly, the absence of defined, enforceable data-sharing protocols across

agencies impedes interoperability. The absence of standardized APIs prevents secure, automated, and efficient data exchange between government bodies and external partners. As a result, data is frequently transferred through insecure channels or duplicated, increasing both costs and risks.

India's Digital Policies on Openness & Interoperability

Policy on Adoption of Open Source Software

The Government of India adopted a formal policy to encourage the use of open-source software in e-governance systems. The policy provides a framework for rapid and effective OSS adoption, ensuring long-term strategic control, reducing vendor lock-in, and lowering the total cost of ownership of digital projects. It is closely tied to the Digital India vision of transparent, efficient, and affordable public services (Policy on Adoption of Open Source Software for Government of India, 2025).

Open API Policy

To promote interoperability, India introduced a policy encouraging the formal use of Open Application Programming Interfaces (APIs) in government systems. This enables integration across applications, supports citizen access through multiple channels, and allows programmatic access for businesses and civil society. The policy strengthens inclusivity and innovation by making data and services more widely usable.

OpenForge Platform

India also launched OpenForge, a government-run collaborative development platform modeled on GitHub. It allows departments to share, reuse, and co-develop e-governance applications.

4. Recommendations and Way Forward

While the Digital Nation Act and the Draft Personal Data Protection Bill contain important and forward-looking provisions, no law is ever permanent. They must be revisited and amended as societal needs, technologies, and risks evolve. Data stewardship is a public responsibility, and protections for privacy and security cannot be sidelined in the push for digitalization. Moving ahead, Pakistan must ensure that frameworks are regularly reviewed, citizen rights are safeguarded, and more actionable datasets are shared openly to support research, innovation, and inclusive governance.

4.1. Legal and Regulatory Reforms

- Swift passage of the Personal Data Protection Law is essential, but with refinements. The bill currently contains vague exceptions such as "national security," "public order," and "public interest," which risk being misused to bypass protections. These terms must be narrowly and precisely defined, and explicit user consent should remain the primary legal basis for all cross-border data transfers. Any exemptions must be made public and transparently justified (Digital Rights Foundation, 2024).
- The proposed National Commission for Personal Data Protection (NCPDP) must be made genuinely independent. At present, its autonomy is undermined by federal government control, ministerial directives, and requirements for government approval before international cooperation. To function effectively, the Commission must be institutionally autonomous, hold its own rule-making authority, be shielded from political directives, and be able to engage internationally without prior approvals.
- The Federal Government's absolute power to make rules and regulations should be curtailed, restoring this authority to the Commission so that data protection standards are set by an independent regulator. Only such institutional autonomy will allow the NCPDP to build credibility and enforce rights consistently.
- Breach notification provisions must also be made stronger and more precise. The bill requires data controllers to notify both the Commission and affected individuals within 72 hours of becoming aware of a breach, but fails to define what constitutes a valid reason for delay. Clear criteria should be set for allowable delays, with guidelines for standardized breach reporting and record-keeping to improve transparency and accountability.
- Parliament should also harmonize conflicting legislation, such as contradictions between the RTI Act and the Official Secrets Act, which create uncertainty around disclosure. To improve legitimacy, open policymaking processes, similar to South Africa's green/white paper system, should be institutionalized, requiring pre-legislative consultation, evidence-based reasoning, and clear public justification of trade-offs.
- The proposed Strategic Oversight Committee (SOC) under the Digital Nation Pakistan Act must also be restructured. While envisioned as an independent body with private sector participation, its credibility is compromised by being chaired by the IT Minister. Independence can only be ensured if no government officials are involved in its leadership.

- Robust legal frameworks must also govern digital ID systems. Citizen data should be classified by sensitivity, with strict protections for biometric, financial, and medical information based on international standards such as the EU GDPR, UK DIATF, HIPAA, and GLBA. Section 29 of the Digital Nation Pakistan Act, which currently provides blanket immunity, should be amended to allow for limited judicial review. Oversight mechanisms must remain independent and accessible, with grievance procedures that safeguard rights and build public trust.
- In the review stage of the Data Protection Bill, the government must facilitate inclusive multistakeholder fora by holding open and transparent dialogue with civil society, experts, and other stakeholders. These discussions should enable the evaluation of current systems and potential implementations across various sectors.

4.2. Data Governance and Standards

- Pakistan must adopt a National Open Data Policy to move from reactive to proactive transparency. Government agencies should be required to publish structured, machine-readable datasets on a centralized portal, with safeguards to protect personally identifiable information. Open data should complement citizens' rights under Article 19A, enhancing accountability, civic innovation, and service delivery. International models such as Indonesia's One Data initiative, India's data.gov.in, and the UK's data portals demonstrate how open data can strengthen inclusive governance and innovation.
- A Data Standardization Policy should mandate harmonized formats, metadata protocols, and interoperability standards across ministries. Adoption of international standards (ISO, W3C, WCAG, XBRL) and mandatory open APIs will reduce fragmentation, enable accessibility, and avoid vendor lock-in. The institutionalization of open-source software adoption would further reduce costs and strengthen digital sovereignty. Global models such as Indonesia's One Data Indonesia, and Estonia's X-Road show how harmonized standards and secure exchange layers can drastically improve system interoperability. Embedding such practices in Pakistan would facilitate government-to-government, government-to-business, and government-to-citizen services

Estonia's X-Road	Indonesia's One Data Initiative
X-Road is Estonia's secure data exchange layer that allows hundreds of independent government and private databases to interoperate. It guarantees interoperability, data integrity, and privacy, saving the state an estimated 1,345 years of working time annually by eliminating redundant paperwork and enabling instant access to reliable data. X-Road is open-source, used internationally (e.g., Finland, Iceland, Japan), and continues to evolve as a model for data interoperability around the world (e-Estonia, n.d.).	Launched in 2019, One Data Indonesia (Satu Data) is a national framework to produce accurate, integrated, and accountable government data. It mandates common standards, metadata, interoperability rules, and the use of reference codes across central and regional agencies. Governance is coordinated by a multi-agency Steering Council that sets policy, oversees implementation, and reports directly to the President (One Data Indonesia, Solution for Data Differences Between Government Agencies, 2022).

- A framework for data minimization is also needed. Sensitive personal data should only be exchanged via secure, real-time APIs with role-based authorization and full logging. The Pakistan Mobile Database (PMD), developed by PTA to restrict SIM and CNIC queries to authorized agencies, provides a practical example. Similar principles of centralized logging, query traceability, and restricted visibility should govern all inter-agency data access.
- A binding legal framework should also define conditions for data sharing among public entities. This must clarify permissible use cases, access rights, roles, and retention periods, while ensuring consistency across provinces given the devolved nature of data governance. Such frameworks must eliminate duplication, insecure transfers, and institutional confusion, while balancing openness with protection.
- Pakistan should urgently establish a National Data Governance Council that brings together key stakeholders, regulators, civil society, private sector, and technical experts, to coordinate national-level data protection strategies. This council must oversee the development of enforceable standards on data privacy, informed consent, and security protocols across both public and private sectors.

4.3. Digital Infrastructure and Innovation

- Reliable connectivity and robust digital infrastructure are prerequisites for transformation. Given fiscal constraints, Pakistan should design public–private partnership (PPP) frameworks specifically tailored to digital infrastructure and services such as e-health, e-governance, and e-agriculture. Alongside PPPs, regulatory sandboxes should be introduced to allow private innovators to pilot new technologies in controlled environments. The Pakistan DEEP initiative, which aims to improve connectivity and digital inclusion, can serve as a foundation for such PPP-driven development.

- The National AI Policy calls for the integration of AI into school curricula, yet thousands of schools across the country still lack functional computer labs. In KP alone, 1,482 government-run schools have no such facilities, raising questions about how AI education can be implemented in the absence of basic digital infrastructure. Moreover, the policy does not account for the rapidly evolving nature of AI, offering no mechanism for updating curricula as technologies chang, an omission that risks rendering educational content outdated soon after adoption.
- The startup and innovation ecosystem must be strengthened to attract investment while ensuring fair competition for local startups against large international technology firms. Incentives should be designed to enable domestic innovators to

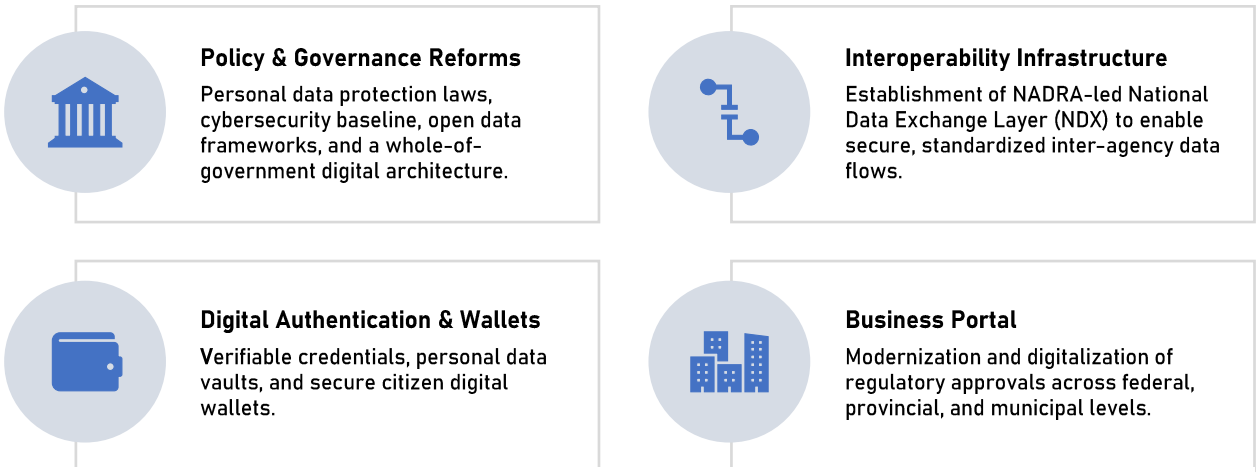

Figure 4: Key components of the Digital Economy Enhancement Project (DEEP)
Source: ("Stakeholder Engagement Plan – DEEP" 2024)

scale, building resilience and reducing dependency on external vendors.

- While the AI Policy outlines measures to expand AI systems and promote innovation, it fails to include provisions for developing machine-learning models in Pakistan's widely spoken languages. Without targeted support for Urdu, Sindhi, Punjabi, Pashto, Seraiki, and Balochi, reliance on foreign-language models will persist, undermining inclusivity and limiting the accessibility of AI tools for large segments of the population.

4.4. Cybersecurity and Trust

- The forthcoming Data Protection Authority should not only enforce compliance but also lead public awareness campaigns on digital rights, literacy, and safe online practices. Pakistan should also invest in indigenous cybersecurity solutions and local manufacturing to reduce dependence on foreign vendors.
- Concerns around surveillance and privacy require clear legal safeguards. Authorization processes must be narrowly defined, with judicial oversight and clear limits on state powers to ensure that security objectives are balanced with fundamental rights.

- A unified cybersecurity governance framework is urgently required. While NADRA's ISO 27001 certification is a step forward, regular independent audits, adversarial testing, and continuous monitoring must become standard practice. National incident-response protocols should also be coordinated across NADRA, PTA, FIA, and provincial agencies to ensure consistency and resilience.

5. Conclusion

Pakistan has the opportunity to transition from a fragmented data governance system to one that is rights-based, transparent, and innovation-oriented. Addressing challenges, ranging from regulatory overlaps and institutional silos to limited enforcement capacity and cybersecurity vulnerabilities will require steady progress on multiple fronts; enacting harmonized legislation, investing in secure infrastructure, enhancing institutional coordination, and promoting responsible and equitable data use are critical next steps. Learning from regional examples and committing to practical, evidence-informed reforms can help Pakistan develop a governance framework that serves its people and supports a more inclusive digital transformation.

6. References

State Bank of Pakistan. (2025). Payment Systems Quarterly Review Q2 of FY25. In *State Bank of Pakistan*. https://www.sbp.org.pk/psd/pdf/PS-Review-Q2FY25.pdf

Global Data Governance Mapping. (2024). Pakistan Data governance. https://globaldatagovernancemapping.org/country-level-data/south-asia/pakistan

LIRNEasia. (2025). Harnessing data for democratic development in South and Southeast Asia - Pakistan. https://lirneasia.net/wp-content/uploads/2025/05/Data-for-development-Pakistan-20250421.pdf

Digital Rights Foundation. (2025). *Digital Nation Pakistan Bill 2024: DRF Analysis and Recommendations*. https://digitalrightsfoundation.pk/digital-nation-pakistan-bill-2024-drf-analysis-and-recommendations/

The Digital Nation Pakistan Bill. (2025). Senate of Pakistan. https://www.senate.gov.pk/uploads/documents/1738057563_368.pdf

Digital Rights Foundation. (2024). Personal Data Protection Bill Summary Table. In *Digital Rights Foundation*. https://digitalrightsfoundation.pk/wp-content/uploads/2024/09/Final-Submission-to-MoITT-by-DRF_Pakistans-Personal-Data-Protection-Bill.pdf

Draft Personal Data Protection Bill. (2023). In *Ministry of Information Technology and Telecommunication*. https://www.moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

Shankar IAS Parliament. (2018). *Global RTI Rating and its flaw*. https://www.shankariasparliament.com/interviews/india-inc/global-rti-rating-and-its-flaw-51

National Archives Act. (2016). National Archives of Pakistan. https://www.archives.gov.pk/ArchivesAct.php

CSIR Open Access Mandate. (2021). In *Google Scholar*. https://scholar.google.com/mandates/csir_in-2021-02-13.pdf

Chakravarty, R. (2017). Open Government Data (OGD) initiative in India. In *Advances in electronic government, digital divide, and regional development book series* (pp. 68–90). https://doi.org/10.4018/978-1-5225-4987-1.ch004

The Legislative process. (n.d.). Parliamentary Monitoring Group | South Africa. https://pmg.org.za/page/legislative-process

Digital Rights Foundation. (2018). *DRF condemns yet another breach of NADRA database and demands strong data protection legislation*. https://digitalrightsfoundation.pk/drf-condemns-yet-another-breach-of-nadra-database-and-demands-strong-data-protection-legislation/

Policy on Adoption of Open Source Software for Government of India. (2025). National Portal of India. https://www.india.gov.in/policy-adoption-open-source-software-government-india

e-Estonia. (n.d.). *X-Road – interoperability services*. https://e-estonia.com/solutions/interoperability-services/x-road/

One Data Indonesia, Solution for Data Differences Between Government Agencies. (2022). Badan Pusat Statistik Provinsi Jambi. https://jambi.bps.go.id/en/news/2022/08/25/278/one-data-indonesia--solution-for-data-differences-between-government-agencies.html

Stakeholder Engagement Plan - DEEP. (2024). In *Ministry of Information Technology and Telecommunication*. https://moitt.gov.pk/SiteImage/Misc/files/DEEP-SEP.pdf

Saxena, A. (2012, September 4). *Indian government launches Data.Gov.In*. MEDIANAMA. https://www.medianama.com/2012/09/223-indian-government-launches-data-gov-in/

Attaa, A. (2018, May 8). Govt officials in Punjab allegedly sold NADRA records, call and police data of Pakistani citizens. *ProPakistani*. https://propakistani.pk/2018/05/07/govt-officials-in-punjab-allegedly-sold-nadra-records-call-and-police-data-of-every-pakistani/

Supreme Court Observer. (2023, October 9). *RTI Judgment: Confusions about Public Interest - Supreme Court Observer*. https://www.scobserver.in/journal/rti-judgment-confusions-about-public-interest/

Profit by Pakistan Today. (2024, July 20). *Pakistan's IT exports up by 24% to $3.2bn in FY24*. https://profit.pakistantoday.com.pk/2024/07/19/pakistans-it-exports-surge-by-24-to-reach-us3-2-billion-in-fy24/

Dawn. (2024, December 9). Pakistan ranked among lowest 12pc globally in mobile, broadband internet speeds in Oct: report. *Dawn*. https://www.dawn.com/news/1877689

Amin, T. (2024, December 18). Talks on 'Digital Nation Bill' inconclusive. *Business Recorder*. https://www.brecorder.com/news/40338210/talks-on-digital-nation-bill-inconclusive

Dilawar, I. (2025, March 28). *Mobile banking, e-wallets drive 12% growth in Pakistan digital*. Arab News. https://www.arabnews.com/node/2595167/amp

Frąckiewicz, M. (2025, August 26). *Pakistan's internet access frontier: fiber optics, 5G delays, and Starlink's big promise*. TS2 Space. https://ts2.tech/en/pakistans-internet-access-frontier-fiber-optics-5g-delays-and-starlinks-big-promise/

Khilji, U. (2025, September 4). Governing AI. *Dawn*. https://www.dawn.com/news/1939562

Raza, S. (2025, September 8). Interior minister forms body to probe SIMs data leak. Dawn. https://www.dawn.com/news/1940395

The Global Data Governance Mapping Project. (2024). Global Data Governance Mapping. https://globaldatagovernancemapping.org/

Annex 1: The Six Attributes of Data Governance Mapping and Their Indicators

Attribute	Definition	Indicators
Strategic	The government has a vision or plan for different types of data in the economy and polity	❖ National Data Strategy ❖ Public Administration Data Strategy ❖ AI Strategy ❖ Strategy for Data in Emerging Digital Ecosystems
Regulatory	The government constructs a legal regime around data's types and/or uses	❖ Personal Data Protection Law ❖ Open Data Law for proactive release of government information ❖ Freedom of Information Law ❖ Right to be protected from Automated Decision-Making Right to Data Portability
Responsible	The government considers ethical, trust, and human rights implications of data use and re-use	❖ Data Charter ❖ Public Sector Data Ethics Framework ❖ Responsible AI Initiatives ❖ Trust Framework for Digital Identity Management ❖ Guidelines for Nongovernmental Data Sharing
Structural	The government alters institutional structures in response to data-driven transformation	❖ Personal Data Protection Body ❖ Open Data Portal ❖ Open Data Coordinating Body ❖ Public Sector Data Governance Body
Participatory	The government informs constituents about its activities and seeks public input with intention to incorporate feedback	❖ Public Consultation on Data ❖ Government Response to Consultation ❖ Multistakeholder Advisory Body

International	The government joins shared international efforts to establish data governance rules and norms	❖ Convention 108+ ❖ Open Government Partnership ❖ OECD AI Principles ❖ Binding Trade Agreements on Cross-Border Data Flows ❖ Budapest Convention

Source: (The Global Data Governance Mapping Project, 2024)

Annex B: PTA's Steps on Data Protection & Cybersecurity

PTA's Steps on Data Protection & Cybersecurity
❖ PTA issued Critical Telecom Data and Infrastructure Security Regulations (2020) requiring all licensees to secure critical telecom data and infrastructure. Measures include automated monitoring systems to detect unauthorized access, steering committees for oversight, clear roles and responsibilities for cybersecurity, employee/contractor training and compliance, physical security of secure areas, strict access controls, disaster protection, and proper maintenance of telecom assets. ❖ PTA has developed a cybersecurity strategy, framework, and audit regime. All telecom operators must undergo regular audits, followed by PTA's independent reviews. ❖ In collaboration with NADRA and other agencies, PTA has set up a task force to investigate data leaks (e.g., NADRA, FBR) and improve controls at 72 collection points. ❖ PTA is developing Pakistan Metadata Database (PMD), a secure application to check CNIC and SIM registration status. Unlike earlier SMS/email systems that were compromised, PMD access will be restricted to provincial police IGs, with every query logged. ❖ A unified framework is being developed to regulate OTT platforms, which collect extensive user data. PTA also enforces social media rules, requiring platforms to establish offices in Pakistan for better cooperation in tracing and enforcement. ❖ PTA has declared its own CII and introduced penalties for violations. ❖ PTA is working with NADRA to enable API-based, real-time verification rather than central data storage. It has introduced 10-finger biometric verification for SIM issuance and random re-verifications, significantly reducing gray SIM misuse.