P@SHA
Pakistan IT Industry Association

Deconstructing Pakistan's Data Governance Draft Policy

P@SHA MEMBER BRIEFING

2026

12 Aug 2026

Authors & Contributors

AUTHORS

Kashoon Leeza — Lead Author
Director, Policy & Strategic Initiatives, P@SHA

Gulraiz Iqbal — Co-Author
Manager, Policy & Govt. Affairs, P@SHA

CONTRIBUTORS

P@SHA Government Relations Committee (GRC)

Sajjad Mustafa Syed — Chairman
P@SHA

Maroof A. Syed — Lead Contributor
President & CEO, CERP

Ahsan Jamil — Lead Contributor
Managing General Partner, SAI Capital

Purpose of this briefing

This document has been prepared for P@SHA member companies and the wider technology industry to assist in understanding the draft National Data Governance Policy 2026 and its practical implications. It is intended as an explanatory resource and does not constitute P@SHA's formal submission to the Government of Pakistan.

1. Introduction

Pakistan's Ministry of IT and Telecommunication released the draft National Data Governance Policy in July 2026.

It is the country's first unified framework for how government bodies collect, protect, and share data. It rests on the premise that public data should be treated as a national asset, and introduces the operating arrangements, standards, and supporting instruments for data interoperability among the government bodies. It is built on six core pillars, detailed in Section 2.

P@SHA's Policy team convened the Government Affairs Committee to review the draft, and conducted a structured survey across the member companies to understand industry feedback on the policy. This briefing consolidates that member input and analyzes the draft against regional and global data governance frameworks. The focus throughout is on the repercussions of this policy for the IT and ITeS industry.

P@SHA views the policy as a building block in Pakistan's digital ecosystem, and in particular as a step that is crucial for the country's Artificial Intelligence (AI) readiness. Member feedback was positive about the general approach to data governance, including the transparency with regard to the use of AI in decision-making, and the emphasis on cybersecurity controls. At the same time, members raised concerns around ambiguity in key definition (such as clarification between public and private data being the most consequential), limited visibility on the security controls and compliance frameworks referenced in the draft, and potential data residency implications for the export sector. Given the policy is still in the drafting stage, the committee's consistent view is that it is premature to draw firm conclusions. However, it is pertinent for the industry to understand the implications of this draft policy.

2. Principal Features of the Policy

The draft policy organizes itself around six pillars. Together they represent the most structurally ambitious data governance attempt Pakistan has made to date.

01 Data rights and stewardship

Custodianship, not ownership

Departments hold data in trust for citizens, not as property

Privacy by design

Citizens can see, correct, and request erasure of their data

02 Technology and infrastructure

AI and cybersecurity governance

AI decisions must be explainable; zero-trust security throughout

Once-only principle and WASL

One record per citizen, shared through a single exchange

03 Institutional and jurisdictional control

Pakistan Digital Authority

Central regulator with binding powers, audits, and enforcement

Sovereignty and openness

Sensitive data stays in Pakistan: non-sensitive data opens up

PILLAR 1. Custodianship, Not Ownership

A conceptual break from the past.

Departments no longer treat the data they collect as their own property. They hold it in trust for citizens.

Duty of stewardship.

Custodianship carries an explicit duty to protect data, maintain its quality, share it lawfully, and disclose it proportionately.

Institutional data-sharing.

This removes the institutional incentive to hoard data in silos, historically a root cause of Pakistan's fragmented government IT systems.

PILLAR 2. AI and Cybersecurity Governance Embedded

Explainability and human oversight.

AI systems used in decision-making must be explainable, continuously monitored, and subject to human oversight.

Public AI registry.

Public bodies would publish automated decision-making systems with significant legal or individual effects in a Pakistan Digital Authority registry, including their purpose, data inputs, and decision logic at an appropriate level of abstraction.

Generative AI specific controls.

The draft includes guardrails against factual inaccuracy, IP violations, and data leakage, an area where it is ahead of most public sector policies globally.

Zero trust and breach notification.

Public bodies must notify the Pakistan Digital Authority (PDA) of data breaches without delay and within the timeline prescribed in a Compliance, Audit, and Certification Instrument. Security controls are to be proportionate to data classification and sensitivity, applying zero trust principles: least privilege, strong authentication, and continuous verification and audit.

PILLAR 3. Once Only Principle and WASL

Sole Authority for data storage.

Agencies must rely on designated Primary Data Registers instead of keeping their own duplicate copies of citizen records.

A governed exchange, not scattered databases.

Data moves between agencies through WASL, a national data exchange platform, rather than ad hoc sharing. This is conceptually closest to Estonia's X-Road, a first for South Asia at this scale.

Zero copy by design.

Duplicate personal data copies are discouraged by design across government systems.

PILLAR 4. Privacy by Design

Privacy-driven governance.

Citizens can see who in government accessed their personal data, when, and why, deniable only on defined legal grounds. This is similar to the EU's GDPR framework, a rare adoption even among global south peers.

Correction, portability, and erasure.

Citizens gain rights to fix inaccurate records, obtain data in machine readable form, and request deletion where legally permissible.

Human review of automated decisions.

Meaningful human oversight is required wherever AI or automated systems make legally significant decisions about a citizen.

PILLAR 5. Institutional Approach

Pakistan Digital Authority (PDA)

A central regulator with power to issue binding directions, run audits, and trigger corrective action for non-compliance.

Chief Data Officers.

A National Chief Data Officer plus a mandatory CDO in every federal public body. All federal bodies will be required to appoint one.

National Data Maturity Index.

An annual, public ranking of institutions on governance, security, data quality, openness, and citizen empowerment.

PILLAR 6. Sovereignty and Openness, Together

Data stays under Pakistan's control.

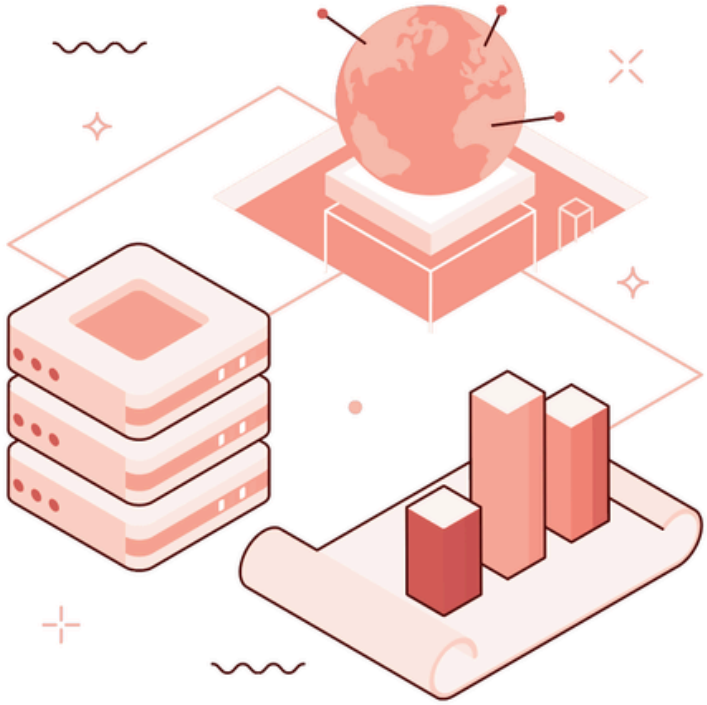
Sensitive government and personal data generally must be hosted and processed within Pakistan. Offshore processing requires prior approval.

Open by default, elsewhere.

Non-sensitive public sector data is to be published via a National Open Data Portal in machine readable form.

Controlled cross border pathways.

Transfers abroad are permitted only through approved mechanisms tied to data classification and jurisdiction. This is intended as the foundation for a national data economy accessed through licensing rather than free export.



3. Data Governance Approach: Global Frameworks

The US, EU, India, and Singapore represent four distinct governance approaches. The table below juxtaposes Pakistan's approach to the global frameworks.

Dimension	Pakistan	United States	EU	India	Singapore
Legal form	Policy, non-binding until gazetted by cabinet	State by state laws/sectoral laws, binding	GDPR + AI Act, binding	DPDP Act 2023, binding	PDPA, binding
Scope	Government data only	Private sector	Public and private	Public and private	Private sector
AI rules	Built in, risk based	Executive order at federal level (AI regulations), Frontier Model Reviews	Separate AI Act	Not yet legislated	Voluntary Advisory Guidelines on Personal Data in Generative AI
Central body	PDA	State AGs, decentralized	Multiple national DPAs	Data Protection Board	PDPC plus sector regulators
Data localization	Required for sensitive/ semi-sensitive data under three-tier approach	None generally	Free flow within EU	Not generally required	None generally

4. Repercussions for the IT and ITeS Companies

Member consultation surfaced a consistent set of structural and definitional concerns. These are the issues most likely to affect day-to-day operations for IT exporters as well as companies working with government clients.

Clarify public versus private data

The draft does not clearly distinguish public data from private data. This matters directly for companies operating in public private partnership arrangements, such as health data arrangements under PPHI.

The policy states that private companies providing services to public departments will be subject to technical controls and audits, but there is limited visibility on what those frameworks actually require. Several member responses independently identified this ambiguity as the single most consequential gap in the draft, since almost every other compliance question in the document depends on how this distinction is ultimately drawn.

Ease data residency requirements

As drafted, the policy applies mandatory in-country residency to all sensitive and semi-sensitive personal data as a general requirement.

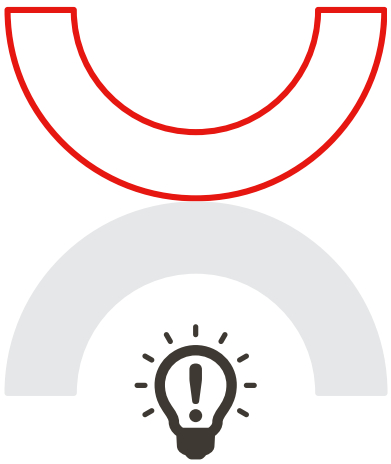
While this applies only to public data, it would still limit access to global cloud platforms, SaaS solutions, cybersecurity services, AI tools, disaster recovery infrastructure, and international technical support. Member feedback consistently flagged this as an area requiring continued attention since a proportionate risk-classification-based approach would ease data hosting requirements especially for semi-sensitive data.

Leverage economic opportunity considerations

Member feedback flagged two sides of the same issue. On one hand, overly restrictive residency and data sharing rules could potentially foreclose legitimate opportunities.

While on the other hand, easing data localization and allowing appropriate access unlocks economic opportunities. Such as Pakistani datasets, for example in health research given the country's high diabetes prevalence, have real value for AI research and could attract foreign investment and research partnership.

5. Open Question(s)



A closer examination of certain provisions of the draft highlights that some areas require further clarity before assessing their applicability in practice.

Data economy versus data stewardship

The draft uses trustee and custodian language for citizens, while simultaneously asserting hard sovereign control at the border. Clause 15.4 states that PDA may prescribe licensing models, pricing principles, attribution requirements, and value capture mechanisms for sharing non-personal public sector data. Licensing and monetizing data is generally understood as something data owners do, not data custodians, so this is a conceptual tension in the draft as written.

Institutional readiness versus implementation

The draft takes a phased approach intended to allow institutional readiness to build over time. The implementation risk is real: the EU's own Digital Omnibus process shows that even mature regulatory regimes can outpace institutional capacity to implement them. Pakistan is proposing to establish a regulator, an exchange, a registry, and a maturity index simultaneously, representing a significant institutional undertaking.

Non-binding versus enforcement

The policy mentioned that public bodies will be audited for their implementation of security controls. However, audits without accountability have remained a weak enforcement mechanism. This is why states like India, Singapore, and the EU all attach financial penalties for non-compliance or failure to report breaches. Whether and how Pakistan's framework will attach comparable financial consequences is an open question. The supporting instruments needed to operationalize enforcement are not yet developed and thus cannot be commented on. Similarly as technology is rapidly changing, audits must take a more proactive approach. On this Singapore's policy merits attention and Islamabad may consider this as a good practice. Singapore updates its AI and data governance guidance every few months rather than legislate a fixed framework.

Data residency versus remote access

The draft defines cross-border transfer to include remote access to government data by persons operating in another jurisdiction. This warrants close attention with regard to access by any member company with freelancers, distributed teams, or Pakistani employees working locally as part of a global company, since the current phrasing could sweep in more arrangements than intended.

6. Recommendations

Clarify scope and residency

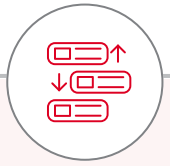
- **Define public versus private data**
  Explicit rules for public-private partnership arrangements
- **Clarify the data classification framework**
  Define tiers, assignment criteria, and who decides
- **Distinguish cross-border access types**
  A time-bound approval path for remote and offshore work
- **Scope rules to government-data processors**
  Not the IT and ITeS export sector as a whole

Protect economic interests

- **Assess export competitiveness impact**
  Before the policy is finalized, not after
- **Harmonize the PDA's mandate**
  Avoid overlap with future data-protection and sectoral regulators

Strengthen AI oversight and enforcement

- **Strengthen AI governance standards**
  Update guidance frequently, following Singapore's advisory model
- **Define fines and penalties**
  For non-compliance and breach-reporting failures



Sequence the rollout

- **Publish an implementation roadmap**
  Binding sequencing plus a regulatory sandbox