Draft National Data Governance Policy

(Recommendations by Digital Rights Foundation)

About Us

Digital Rights Foundation (DRF) is a women-led, not-for-profit organization working since 2013 to advance digital rights and online freedoms across South Asia and the broader Global Majority. We advocate for inclusive, rights-respecting digital spaces by driving policy change through strategic engagement with relevant stakeholders. Our work focuses on making digital platforms and emerging technologies more equitable, accessible, and accountable. At the grassroots level, we empower individuals, particularly women, marginalized communities, and human rights defenders, with the tools and knowledge to navigate the Internet safely and assert their rights online.

For more information, visit:

www.digitalrightsfoundation.pk

Submitted by: Digital Rights Foundation

Dated: 13.07.2026

DIGITAL RIGHTS FOUNDATION

DRAFT NATIONAL DATA GOVERNANCE POLICY

(RECOMMENDATIONS BY DIGITAL RIGHTS FOUNDATION)

Data has become one of the most consequential assets a modern state administers. As Pakistan's public sector increasingly digitises citizen services, shares information across departments, and builds interoperable systems to strengthen governance, the manner in which the State collects, stores, shares, and protects data about its citizens will directly shape public trust, service delivery, and the practical realisation of the right to privacy under Article 14 of the Constitution of Pakistan, 1973. Given this, a national data governance framework is not merely a technical or administrative undertaking; it determines whether digitisation strengthens the relationship between citizen and State, or further exposes citizens, particularly the most vulnerable among them, to new and significant risks.

Digital Rights Foundation (DRF) welcomes the Ministry of Information Technology & Telecommunication's (MoITT) development of the Draft National Data Governance Policy 2026 ("Draft Policy") as an important step toward establishing binding national direction for public-sector data governance, and recognises the Ministry's commitment to open consultation on this framework. DRF also acknowledges the strengths of the Draft Policy, including its framing of Government data as held in trust for the people rather than owned by the State, its adoption of privacy-enhancing technologies such as zero-knowledge proofs and selective disclosure, its proposed algorithmic-transparency registry for automated decision-making, and its recognition of a citizen's right to meaningful human review of automated decisions.

Having reviewed the Draft Policy in detail, and drawing on comparative regulatory practice and DRF's experience working on digital rights and data protection in Pakistan since 2013, DRF has identified critical gaps in the Draft Policy, particularly around regulatory independence, sequencing relative to Pakistan's pending data protection legislation, federal-provincial implementation, and protections for vulnerable groups, and submits the following

recommendations to ensure the Policy delivers a data governance framework that is both effective and rights-protective.

A. QUESTIONNAIRE FOR STAKEHOLDER FEEDBACK AND CONSULTATION

As part of this consultation, the MoITT circulated a questionnaire seeking stakeholder input on ten areas;

1. What do you think are the major challenges currently hindering effective data governance, interoperability, and data sharing within Pakistan's public sector? *(Examples: siloed infrastructure, lack of standardized formats, privacy concerns, inadequate technical capacity, legal ambiguities, or others)*

2. Which areas of citizen data empowerment and privacy protection should be prioritized to build public trust? *(Examples: granular consent mechanisms, transparency in automated decision-making, ease of data correction/erasure, privacy-enhancing technologies) The policy proposes specific data residency tiers (e.g., mandatory in-country hosting for Restricted/Personal data, and governed offshore processing for other tiers).*

3. How effective and practical do you think these data sovereignty mechanisms will be? What additional safeguards or flexibilities would you recommend?

4. How can the government ensure equitable access to "Open Data" for researchers, startups, and marginalized communities to foster innovation while preventing misuse? *(Examples: accessible National Open Data Portals, API availability, localized/translated datasets, targeted awareness programs)*

5. What role should the private sector, academia, and civil society play in collaborating with the National Data Governance Council (NDGC) and the Pakistan Digital Authority (PDA) to implement this policy?

6. What kind of compliance, audit, and grievance redressal mechanisms are necessary to ensure public bodies adhere to the "Privacy by Design" and "Once-Only" principles?

7. How can collaboration and data exchange between federal public bodies and provincial governments be improved through the National Data Exchange (WASL) and designated Primary Data Registers?

8. What monitoring and evaluation frameworks or metrics (such as the proposed National Data Maturity Index) would be most useful to assess the compliance and progress of public bodies?

9. Are there any specific regulatory incentives, technical support, or capacity-building programs that should be introduced to help public bodies and contractors transition to this new data governance architecture?

10. Please share any additional thoughts, suggestions, or concerns regarding the Draft National Data Governance Policy.

B. RESPONSES TO THE CONSULTATION QUESTIONNAIRE: KEY CONCERNS AND RECOMMENDATIONS

The following section sets out DRF's responses to each of the consultation questions circulated by the MoITT. It identifies the key legal, policy, and governance concerns from the Draft Policy and provides recommendations to strengthen the proposed framework in line with international best practices and Pakistan's constitutional and institutional context.

I. KEY CONCERNS AND GAPS IN THE DRAFT POLICY

1. Challenges Hindering Effective Data Governance, Interoperability, And Data Sharing Within Pakistan's Public Sector

- One of the biggest challenges facing the government sector in Pakistan when it comes to safe, easy, and effective data governance is the lack of security protocols. Data breaches of national datasets occur on a consistent basis, with the most recent case happening just 2 weeks ago at the Capital Development Authority (CDA). Just at the beginning of this year, the government held a standing committee that discussed the involvement of public sector employees in stealing and selling citizen data online on the dark web.

- Digital systems are fraught with holes that can easily be identified and exploited for private gain, either by non-state actors or other states who would benefit from disrupting data operations in Pakistan and gaining access to private, personal, and identifiable information on Pakistani citizens

- This lack of efficient and effective security structures in place, alongside the fact that a detailed personal data protection law is still in the process of being passed and/or finalized, makes the challenge twofold. Not only does it make databases vulnerable to attacks from third parties and non-state actors, but making the data available for sharing across departments or government bodies also increases the likelihood of data leaks, loss of data, or the use of data for unauthorized purposes.

- Another challenge that presents itself is the lack of public employees who have the requisite training or understanding of how to deal with and/or manage personal data once collected. Without a proper understanding of data governance, the importance of data protection, as well as the ways in which data should be collected from citizens, the implementation of this policy, which relies on collecting accurate and fit-for-purpose information, would be highly difficult, especially when it comes to provision for privacy.

- Additionally, while the policy states that all provinces will operate under 'harmony' with the PDA, many departments in remote or rural areas still rely on outdated, paper-based models that operate in isolation. Without a standardized digital structure in place, which includes hardware, software, as well as access to digital tools such as the internet, the policy would not only be inapplicable but would cause massive loopholes in regions where citizen vulnerability is already high because of their distance from more centralized, urban hubs of government.

- The significant legal challenge is that the Draft Policy is being built on a foundation that does not yet exist. The Draft Policy abbreviation lists *the* Personal Data Protection Law ('PDPL') as the anticipated law. Clause 11.3 of the Draft Policy provides that data-subject rights *"shall be recognised and given effect as provided by applicable personal data protection law"* and that the Draft Policy *"shall be updated to align with the statutory regime once the Personal Data Protection Law is enacted"*, and that where such law is "*more protectiv*e" than the more protective provision prevails.

- However, in reality, Pakistan has never enacted a dedicated data protection law. The PDPB has been through multiple drafts and public consultations since 2018 without passage, with unresolved concerns over the scope of consent, cross-border transfer rules, and the independence of the proposed regulator. Consequently, the Draft Policy's entire rights architecture, such as lawful basis (clause 11.2), granular consent (clause 12.2), access transparency (clause 12.3), rectification and erasure (clause 12.7), and breach notification to the authority designated under the personal data protection law (clause 11.8), is drafted by reference to a statute and a regulator that do not currently exist. This

means the enforceability of every citizen-facing right in Sections 11–12 is legally contingent on future legislation whose timeline and final content are uncertain.

- The absence of a data protection framework is compounded by the absence of any independent data protection authority. The proposed National Commission for Personal Data Protection exists only as a prospective body under the pending Bill, and clause 16.9 of the Draft Policy itself concedes that *"the supervision of personal data processing as a matter of data subject rights is the function of the authority designated under the personal data protection law"*, a function Pakistan Digital Authority ("PDA") expressly disclaims for itself. This leaves a live regulatory vacuum as there is presently no independent body empowered to set enforceable data-protection standards, lawful processing obligations, investigate breaches by public bodies, adjudicate citizen complaints, or impose penalties for mishandling of personal data, and PDA's own mandate under this Draft Policy is limited to data governance as a national asset rather than data-subject rights supervision.

- **C**omparative experience further illustrates the risk of proceeding with large-scale data infrastructure ahead of a functioning privacy law. In Kenya, the High Court halted the Huduma Namba digital-ID rollout in 2021, and again paused its successor Maisha Namba in 2023, in both cases for lacking a mandatory Data Protection Impact Assessment. In Jamaica, the entire National Identification and Registration Act 2017 was declared "null, void and of no legal effect" in Robinson v Attorney General of Jamaica (2019) for insufficient privacy safeguards. Given that Article 14 of Pakistan's Constitution guarantees "the dignity of man and, subject to law, the privacy of home," operationalising WASL and Primary Data Registers before a PDPB and independent regulator exist raises comparable constitutional exposure.

2. **Priority Areas for Citizen Data Empowerment and Privacy Protection To Build Public Trust**

- Building public trust around data collection and storage and other data governance operations requires giving individuals control over their personal data, offering transparency at all levels, and following privacy by design protocols.

- Research shows that privacy by default, which offers proactive and preventative procedures, helps create informational ecosystems that allow governments to deal with the complex nature of collecting, storing, and using personal data. Although the drafted policy does list a commitment to privacy-by-design protocols, it should be followed by or accompanied by strict security systems that tackle the ongoing problem of data breaches in major government departments.

- Similarly, following General Data Protection Regulation (GDPR) guidelines for consent gives citizens the leverage to manage their data and control the information as needed. Dynamic informed consent, i.e., consent that allows citizens to actively manage, update, and monitor their information in real time, can also help citizens have an added layer of protection by not only giving them access to their data and the chance to delete or modify it, but also to track its use and the flow of data within larger processes.

- Transparency in data collection processes is equally important when building public trust around data governance. Clearly explaining and laying down why this information is being collected, how it will be stored, where it will be stored, who will have access to it, and who it will be shared with. This is especially important given the fact that the policy has laid out the possibility of citizen data being used to train or inform AI models, which can complicate data privacy and trust. This would also include making clear to citizens which residency tier their information is falling under and why it's necessary to process it under offshore or cross-border facilities.

- It would also allow for citizens to exercise their right to information from any government department at any time. While the policy, as it is drafted at the moment, has made provisions for this under the Right to Information Act (RTI), studies show that most RTI processes function poorly, with information requests mostly being met with silence.

- Following from this, citizens should be given the right to withdraw consent from having their information used to inform models of emerging technologies. It should be noted that all information-sharing documents given to citizens should be written up in simple language without unnecessary legal or technical jargon. They should also be available in a number of languages to be accessible to all individuals.

- Children's data protection also requires stronger treatment than the draft currently provides. Clause 11.6 of the Draft Policy states that data relating to children shall receive "enhanced protections," including a specific lawful basis, age-appropriate notice, and parental or guardian engagement "where required," but the Policy does not specify age-verification mechanics, parental-consent workflows, or how children's data is to be treated within the residency and citizen-rights architecture more broadly. This is an internal consistency because Pakistan's own draft Personal Data Protection Bill, under clause 14, already holds children's data safeguards in better terms, so the Policy should be aligned with those protections.

- In the context of generative AI, citizens should be allowed to refuse inclusion or processes under such systems without fearing prosecution, suspicion or exclusion from public goods and/or services.

- But to ensure that all provisions made to build trust and create privacy provisions, means citizens should be educated to understand their privacy rights, what risks can be posed when providing information, and how to recognize scams from hackers or private actors trying to farm information for private gain. This means having awareness campaigns in schools, offices, and on social media to inform citizens about their rights

and how they can be exercised as well as guiding them on how and where proper, detailed information can be found. Information helplines and kiosks manned by local civil servants should also be made available in all provinces and major cities to ensure that no region or area is left out of accessing and understanding vital information.

- Another aspect of public trust involves assuring citizens, especially vulnerable ones, that their information will not or cannot be accessed by family members or acquaintances without prior consent or warning. At the moment, family members can visit NADRA centers and request information on any family member, regardless of whether prior consent is given by said member. As the policy is currently drafted, the existence of centralized registers and access logs poses acute risks for women and minority groups whose information can be downloaded and exploited by family members. These risks become even more dangerous if and when women and gender minorities belong to abusive households or have survived situations of gender-violence. Legal precedents from the UK and Australia show how important it is to have proper safeguards built into processes such as WASL to allow for confidentiality against relatives and family members who can pose harm.

3. **Effectiveness And Practicality Of Data Sovereignty Mechanisms: Additional Safeguards Or Flexibilities**

- The tiered residency model (clause 8.2) is well-designed as it differentiates obligations based on the sensitivity of data, for example, imposing stricter controls on sensitive personal data while allowing flexibility for open or non-sensitive data. This model reflects the EU's risk-based approach under the GDPR, particularly under Articles 24, 25, 32, and 35, which require compliance measures to be proportionate to the risks associated with different types of data processing. Also, Trust-not-ownership framing under clauses 5.2 and 11.1 gives personal data fiduciary status, which is also strong wording, as it means authorities can't treat citizen data as a proprietary asset.

- However, the infrastructure doesn't yet exist in Pakistan to match the ambition of the Draft Policy. The Tier 1 of the Draft Policy mandates in-country hosting for all sensitive personal and authoritative source data of national importance, but does Pakistan have sufficient domestic data-center capacity, and cloud infrastructure is an important concern. If that capacity doesn't exist at scale, authorities either don't comply or comply with under-resourced infrastructure that creates risks for security greater than a foreign cloud would. Furthermore, the Draft Policy also fails to consider practical requirements, such as the lack of electricity and energy supply in order to run such data centers. In a context where Pakistan already does not have the resources to meet current energy requirements, with local industries suffering due to load-shedding and unreliable electricity supply, regular nationwide grid failures, and natural disasters, data localisation does not seem to be practically implementable.

- The Draft Policy's approach to cross-border transfers is a strong safeguard for protecting government data. However, the concept of "material remote accessibility" in Clause 3.5 is too broadly defined. It is unclear whether it includes activities such as remote technical support by a foreign engineer or the use of SaaS platforms with administrative functions hosted outside Pakistan. Such ambiguity could result in inconsistent implementation, and some authorities may use the provision too narrowly, while others restrict legitimate operational practices.

- For Foreign-jurisdiction access, Clause 8.4 says *"notify PDA, shall not voluntarily disclose, and shall comply only as permitted by Pakistani law and applicable mutual legal assistance arrangements"* but this does not address what happens when a foreign law conflicts with Pakistani law.

- The Draft Policy gives the PDA multiple roles, including issuing the rules (Clause 13.3), granting the approvals (Clause 8.2), getting notified of breaches (Clause 11.8), and enforcing corrective action (Clause 18.5), all with no independent oversight or appeals mechanism.

- The Draft Policy just encourages the Provincial governments to adopt it or equivalent frameworks under clause 7.2 rather than mandating implementation of binding frameworks, which contradicts the "federation as architecture" in clause 5.5. A federated data sovereignty regime needs binding minimum standards for provinces not just *"encouraged to adopt"* through the NDGC, so as to ensure consistent implementation of the Draft Policy.

- Enforcement provisions are also weak. While the Draft Policy empowers the PDA to issue binding directions (clause 16.2) and corrective action (clause 16.1), it does not prescribe a clear penalty schedule, administrative fines, or accountability framework for non-compliance. In contrast, the GDPR provides an enforcement regime under Article 58, which empowers supervisory authorities to issue binding orders and corrective measures, while Article 83 GDPR establishes significant administrative fines based on the nature, duration and gravity of the infringement. Without such meaningful financial or regulatory consequences, compliance may lose priority.

4. <u>Ways To Promote Equitable Access to Open Data While Preventing Misuse</u>

- Before going into how open data access for professionals in the private sector should be established, it's important to understand that open data initiatives are largely meant to be open for everyone, including citizens, to allow for societies to hold governments accountable and to allow for true transparency.

- That being said, open data access should not only be made available to researchers, startups or marginalized groups but also follow an 'open by default' principle where anyone can access data collected by the government.

- According to the International Open Data Charter, in order for open data to be accessible and effective, it should follow 8 key principles which allow data to be: open by default, timely and comprehensive, accessible and usable, comparable and interoperable, for improved governance, and for inclusive development and innovation.

- To that effect, to ensure that open data initiatives made by the government offer equitable access to all potential users, it needs to be available on a central portal or database that is easily discoverable online by anyone who has internet access. Data also needs to be available in a format that's available to the widest range of users, meaning that it should not be on platforms or in data files that can only be opened or used by people who have specialized access to certain digital tools. Access to data should also be free of cost and not behind a paywall of any kind, and should not require a license for use.

- To further ensure that everyone has equal access to open data provided by the government, the data should be made available in languages that are understood by a majority of the population, which can include but should not be limited to Urdu, Sindhi, and/or Pashtu. To allow for true equal access, individuals should also be given the chance to take part in training and learning sessions that teach them how to access, safely use, and handle open data. This is especially true for women in Pakistan, who are especially impacted by lower digital literacy rates, and for individuals residing in rural or remote areas of Pakistan. Targeted programs that teach students as well as professionals the availability of open data, the importance of it, as well as the ways in which it can be used and what standard of care needs to be kept in mind when using it will ensure that there isn't any isolated data usage.

- Given this, it is understandable that not all data available to the government can be made public due to privacy and security concerns. This applies equally to sensitive data that might compromise ongoing government operations or that can be used against the government, as well as personal identifiable information that the government holds about citizens. For example, open data should not publish names, identity card numbers, addresses, phone numbers, or other personal information about the citizens of Pakistan. Estonia's data retention policy offers a great example of how not all metadata needs to be logged or retained by governments and made accessible to the public. Metadata that cannot be aggregated into profiling systems or used under mass

surveillance tools should be given priority rather than any and all information. As set out by the Estonian government, mass data retention "breaches trust between citizens and the state and thus should not be used in a democratic society."

- There are other risks of establishing open data. Research conducted by the OECD states that risks of open data can go beyond primary security breaches into domains of violation of privacy and intellectual property theft, limitations of anonymisation, amongst others. To counteract these risks, the government needs to establish risk management models that put privacy at the center of every design and implementation process.

- Classifying data sets according to the risk they present can protect sensitive information from falling into the wrong hands while ensuring that the relevant professionals and individuals can gain access to the relevant data as needed.

5. **Role of the Private Sector, Academia, and Civil Society in Implementing the Draft Policy**

- As currently drafted, clause 16.5 of the Draft Policy allows PDA to designate *"such other public, private, academic, or civil-society members as PDA may designate from time to time"* to sit on the NDGC, meaning participation by these stakeholders is entirely discretionary, revocable, and ad hoc rather than a guaranteed institutional right. This is an important governance gap given the Council's functions, as it advises on the designation and custodianship of Primary Data Registers, reviews the National Data Maturity Index, and shapes the National Data Strategy (clause 16.5), all matters with direct consequences for citizens, researchers, and industry. This is further compounded by the fact that PDA simultaneously chairs the Council, issues the standards the Council reviews, and audits compliance with those standards, with no independent oversight body named anywhere in the draft. Brazil's National Council for the Protection of Personal Data and Privacy (CNPD) offers a workable precedent. The council has 23 members, 12 of whom are non-government, including industry, academia, and civil society, with that

representation guaranteed by statute under Articles 58-A/58-B rather than left to regulatory discretion.

- Beyond Council membership, each stakeholder group's most legally coherent role lies in the specific instruments the Draft Policy already contemplates. The private sector's involvement is channeled through the public-private data partnerships (clause 15.2) and recognised data trusts/intermediaries (clause 15.3), both currently authorised at PDA's discretion under a yet-to-be-issued Data Value and Re-Use Instrument. There is presently no standard contractual framework governing these arrangements, only a broad reference to future fiduciary, security, and conformance requirements. To address this, they should instead be governed by published, standardised contractual templates addressing fiduciary duties, audit rights, and data-return obligations, rather than case-by-case authorisation, to prevent inconsistent bargaining outcomes between government and private partners of unequal size and leverage.

- Academia is best positioned to contribute independent technical scrutiny of de-identification and Privacy-Enhancing Technology methodologies (clauses 12.4 and 12.5) and to the AI-ready data programme (clause 14.3), both of which currently sit entirely within PDA's own determination with no external validation mechanism specified.

- Civil society's most valuable formal contribution is oversight of the citizen-facing redress ecosystem. For instance, a nominated observer or advisory role within the Rights Handling, Notices, and Redress Instrument (clause 11.7), and mandatory participation in the public consultation the Draft Policy requires for "*material amendment*s" under clause 18.6, a safeguard currently weakened by the open-ended exception "s*ave where urgency requires otherwise*," which should be narrowed and clearly defined to prevent it from becoming a routine bypass of stakeholder input.

6. **Ensuring Compliance with the Privacy by Design and Once-Only Principles**

- As drafted, "Privacy by Design" (clauses 6.10 and 12.4) and the mandatory Privacy Impact Assessment for high-impact processing (clause 11.4) read as documentation obligations rather than pre-deployment gates. The Draft Policy does not state anything about the completion and approval of a Privacy Impact Assessment ('PIA') before processing sensitive or high-impact personal data. For the Once-Only principle, compliance currently has no verification mechanism beyond what each public body chooses to report.

- Verification of both principles requires independent checking. A two-tier audit model is appropriate: routine PDA-led reviews for standard-risk systems (consistent with clause 18.4), and mandatory, externally commissioned third-party audits for high-risk or Tier 1 systems, since PDA's dual role as both standard-setter and auditor creates an inherent independence concern. Audits should specifically test whether the PIA preceded deployment and whether the agency is genuinely drawing from the authoritative source rather than re-collecting citizen data, with findings published in meaningful form rather than reduced to a single score.

- The complaint mechanism also needs to be easily accessible, particularly given that citizen data is already in a vulnerable position due to the absence of an enacted data protection law and regulator. Complaints should be classified by the nature of the query for instance, being asked to resubmit information the government should already hold under the Once-Only principle (clauses 6.6, 10.7) should be its own distinct category, since clause 11.7 as drafted, is oriented toward personal-data rights (access, correction, erasure) and does not clearly capture this scenario.

7. **Federal–Provincial Collaboration In the National Data Exchange (WASL) and Primary Data Registers**

- One of the major issues reflected in the Draft Policy, by its own terms, binds only federal public bodies under clauses 7.1 and 7.2, while provincial governments are merely to be

coordinated with and encouraged to adopt this Draft Policy or equivalent frameworks. This is a major issue because many of the data sets relevant to Primary Data Registers (clause 6.4A), such as land records, local civil registration functions, and provincial revenue and licensing data, fall within provincial or concurrent legislative competence following the 18th Amendment.

- The Draft Policy is also silent on liability allocation across the federal-provincial boundary. Clause 6.4A places accountability on "the custodian public body," but does not address what happens when an error originating in a provincial register propagates through WASL and harms a citizen relying on a federal service. There is likewise no dispute-resolution mechanism for conflicts between overlapping federal and provincial datasets covering the same subject matter (e.g., competing identity or domicile records).

8. Monitoring And Evaluation Frameworks To Assess The Compliance And Progress Of Public Bodies

- Relying on annual self-assessment for all public bodies (clause 19(a)) is a weak evidentiary basis for an index meant to "inform corrective action, prioritisation, and recognition" (clause 18.3). Verification should instead be tied to the same risk tiers the Policy already uses for residency (clause 8.2), applying the Policy's own proportionality principle (clause 6.14) to compliance monitoring, and concentrating independent verification where the risk of harm is highest.

- Clause 18.3 provides that National Data Maturity Index (“NDMI”) results shall be published annually and shall inform corrective action, prioritisation, and recognition, but it does not specify the criteria or methodology used to determine those results. Publishing the underlying methodology would create greater transparency and build public trust regarding data protection and accountability, and would allow a public body to understand and, where necessary, contest the basis of its own score before any corrective action is taken against it.

- In addition to this, in the event of data breaches, leaks, or other unfortunate circumstances, relevant and responsible government departments should create incident response reports that detail the events, the reason for the violation, a reevaluation of data systems and processes, as well as what redress mechanisms were employed should be written down in detail. Furthermore, the reports should be made public and accessible to technical, academic, and CSO experts for independent review.

- All frameworks made under the policy should be exposed to and available for external and independent review by industry experts within Pakistan to ensure that the models and frameworks in place are prioritizing citizen data, citizen privacy, and security.

9. <u>Regulatory Incentives, Technical Support, Or Capacity-Building Programs To Help Public Bodies And Contractors Transition To This New Data Governance Architecture</u>

- Technical support in the form of basic infrastructure that can handle large volumes of data and that allows for the standardization of processes should be provided to all departments at all levels of the data governance chain. This includes access to the internet, access to functioning and modern computer equipment, alongside more specific support such as tools used for data cataloging, data quality, and master data management. Other technical support includes software that allows for metadata registries and secure data-sharing platforms. Proper data architects should be hired to provide this kind of support and to advise teams on best practices for data governance. Such IT teams should also be encouraged to man and manage a help desk for IT departments across the country to troubleshoot incoming problems as well as to support citizen needs and questions.

- Capacity building programs should be implemented with role-specific training, especially for senior executives, data officers and monitoring and evaluation teams, as well as IT professionals responsible for handling and safeguarding this information.

- All public officials involved in the data governance process should obtain data governance certification, such as the one offered by ISACA, to make them better equipped to understand the data they're required to protect as well as understand the possible risks and how to deal with them. In addition to this, regular workshops and webinars should be held with experts in data governance, data privacy, and data management, which can help officers better gauge how to implement the data governance process in the most accurate, efficient, and safe manner.

- To make all this possible, the government needs to offer proper financial support to departments in underdeveloped regions and low-funded provinces to ensure that no one gets left behind and that all processes are standardized across the data governance structure. The government should allocate dedicated funds and resources for regular system upgrades, necessary equipment, staff training programmes and cybersecurity enhancements.

- Most importantly, the government should establish independent and third-party-ruled oversight for this data governance process to check implementation and rollout, and also to flag any incoming problems, concerns, questions about unnecessary processes, or violations should they take place. This oversight board or committee should be allowed to conduct periodic, random checks and reviews of departments.

10. Additional Thoughts, Suggestions, Or Concerns Regarding The Draft Policy

- The Draft Policy's reliance on the anticipated PDPB is premature, since it has not yet been enacted into law. Until it is passed, any policy built on its assumed provisions risks becoming yet another unimplemented framework, because it will depend on legislation that may never exist in its current form. It is therefore important that the PDPB itself be enacted as law before the Draft Policy relies on it as a governing instrument. Furthermore, Pakistan's proposed PDPB has been criticised for falling short of the standards set by the EU's GDPR, particularly around the independence of the proposed regulator, the scope and specificity of consent requirements, and fixed enforcement

timelines. Since GDPR is already cited in this Draft Policy's own Bibliography (b-4) as an informing instrument, adopting its core standards more explicitly in the upcoming PDPB would provide stronger legal backing for this Draft Policy's data governance framework and help ensure that the PDPB meets internationally recognised benchmarks rather than replicating the gaps of the current Bill.

- The national security carve-outs made by the Draft Policy under Clause 7.4 are too broad and vague in nature and fail to take into account how easily they can be exploited to target or attack especially vulnerable groups in Pakistan, such as minority ethnic and religious groups, journalists, human rights defenders, and lawyers. The DRF has made the same point about broad "national security","public interest" exemptions in PDPB as well because such exemptions often enable risks of unchecked surveillance and unauthorized data collection/sharing, which can put the safety and identity of people at risk.

- The Draft Policy's own bibliography cites Saudi Arabia's Saudi Data and Artificial Intelligence Authority (SDAIA)/National Data Management Office (NDMO) framework as an informative instrument. We recommend engaging this citation explicitly as a cautionary comparator. SDAIA reports directly to the Prime Minister; its NDMO oversees data-governance standards while SDAIA enforces the PDPL, i.e., standard-setter, operator and enforcer fused, with no independent regulator. The Pakistani architecture mirrors this SDAIA model. Such a structure risks importing the least rights-protective element of the frameworks it cites while omitting Estonia's institutional independence and Australia's separation of functions.

- Under the Data Availability and Transparency Act 2022 of Australia, government data sharing is regulated by the Office of the National Data Commissioner (ONDC), while privacy and freedom of information oversight remain the responsibility of the Office of the Australian Information Commissioner (OAIC). The two are governed by a published Memorandum of Understanding, the Act expressly states that it "does not override the Privacy Act 1988," and sharing must be consistent with it. The scheme also maintains

public registers of accredited participants and data-sharing agreements and publishes annual reports, promoting transparency and accountability. Similarly, Estonia's X-Road framework, which is already cited in the Draft Policy, provides a similarly instructive example. Operated by the Information System Authority (RIA) together with the Nordic Institute for Interoperability Solutions (NIIS), X-Road facilitates secure interoperability while maintaining a clear institutional separation between digital infrastructure management and privacy oversight. Rather than centralising data, each public authority retains control over its own databases, while independent privacy supervision is exercised by Estonia's Data Protection Inspectorate (AKI). Per RIA and GovInsider's Digital Public Infrastructure special report, X-Road *"facilitates over 2.2 billion transactions annually and powers more than 3,000 digital services,"* with over 95% of Estonians using e-services and 99% of government contacts conducted online. Pakistan should adopt a similar institutional framework to strengthen accountability, reduce conflicts of interest, and enhance public trust.

- It is worth acknowledging, in closing, that the Draft Policy also contains genuinely strong provisions worth preserving as the framework develops including the zero-knowledge-proof and selective-disclosure provisions (clause 12.5), the algorithmic-transparency registry for automated decision systems (clause 14.5A), the "held in trust for the people" fiduciary framing of citizen data (clauses 5.2, 11.1), and the right to meaningful human review of automated decisions (clause 12.9). These reflect genuinely rights-protective design choices, and the recommendations above are intended to build on that foundation rather than to displace it.

II. RECOMMENDATIONS AND FEEDBACK

- Do not operationalise WASL, Primary Data Registers, or the citizen-rights chapter (Sections 11–12) until the PDPB is enacted and an independent data-protection authority is functioning, as this is a constitutional-risk issue, not merely a sequencing preference.
- The absence of enforceable data protection also carries a distinct constitutional-risk dimension where biometric data is concerned - biometric identifiers should be treated as a distinct, heightened-sensitivity category.
- Create awareness campaigns on citizen rights under data governance, so that consent, access, correction, and erasure rights are understood and usable in practice, not just formally granted.
- Strengthen and standardize RTI processes to ensure timely and accurate responses.
- Employ proper channels of consent that allow citizens to accept or reject any data processing, collection, or retention requirements, where possible
- Make data collection and processing mechanisms transparent using simple and easy language.
- The Draft Policy should adopt a phased approach to Tier 1 data residency, linking mandatory localisation requirements to the development of adequate domestic data centre and cloud infrastructure. Until sufficient national capacity is established, it should permit Tier 1 data to be processed on trusted foreign infrastructure, provided the data is encrypted with Pakistan-held encryption keys, processed in accordance with security standards, and subject to periodic review as domestic infrastructure develops.
- The Draft Policy should clearly define the thresholds for "material remote accessibility" by specifying objective criteria, such as the level of access granted, the ability to view or extract data, the persistence or duration of access, and the volume or sensitivity of data involved. This would promote consistent implementation while ensuring that legitimate operational activities are not unnecessarily restricted.

- The Draft Policy should include a conflict-of-laws framework to guide public bodies in responding to foreign legal demands that conflict with Pakistani law, along with requirements for notification, review, and reliance on mutual legal assistance mechanisms.

- For better accountability and public trust, the Draft Policy should establish an independent review or appeals body, such as an appellate panel, to review PDA designated roles and decisions.

- The Draft Policy should establish binding minimum data governance standards through a negotiated intergovernmental framework in accordance with the 18th Constitutional Amendment while ensuring consistent implementation across federal and provincial governments. The NDGC should serve as the platform for developing and coordinating this framework in collaboration with provincial governments.

- The Draft Policy should introduce a proportionate enforcement framework that includes administrative and financial consequences for non-compliance, supported by transparent enforcement procedures. Such a framework should ensure that sanctions are proportionate to the nature, severity, and duration of the breach and should promote accountability and consistent implementation across public bodies.

- Use "open by default" principles and confirm it applies to the general public, not only named user categories.

- Make data available in regional languages to ensure that all citizens can understand and interpret information as needed

- Provide academic and professional institutions with proper training sessions that explain how open data can be used, what SOPs should be followed when handling open data, and how safety can be ensured

- Account for risks posed by open data, such as familial access to private information and limitations of anonymisation, by having routine risk assessment/management models.

- Embed a structured risk-classification framework at the dataset design stage, not only before release.
- Private-sector, academic, and civil-society representation be converted from a discretionary PDA appointment to a non-discretionary seat allocation, for example, through a transparent nomination or rotation process, all in line with the accountability and transparency principles that the Draft policy itself professes in clause 6.15.
- Govern public-private data partnerships and data trusts (clauses 15.2, 15.3) through published, standardised contractual templates addressing fiduciary duties, audit rights, and data-return obligations, rather than case-by-case authorisation.
- Establish a nominated civil-society observer role in the Rights Handling, Notices, and Redress Instrument (clause 11.7).
- Narrow clause 18.6's "urgency" exception to a defined, enumerated set of circumstances, with mandatory post-hoc consultation.
- Every public body should be legally required to complete and obtain sign-off on a PIA before any system involving high-impact or sensitive personal data processing goes live, with mandatory reassessment whenever the system's purpose, data linkages, or user base expands materially. This should be paired with a mandatory, standardised Data Protection/Privacy checklist fixed into the public procurement and system-design lifecycle so privacy controls are incorporated at the design stage rather than rebuilt afterwards.
- Mandate an annual Agency CDO attestation, backed by verifiable usage records, that the body is consuming from designated Primary Data Registers rather than re-collecting citizen data.
- Adopt a two-tier audit model: routine PDA review for standard-risk systems, mandatory external third-party audit for Tier 1/high-risk systems, with findings published in full rather than as a single score.

- Add a distinct, fast-tracked (15–30 day) complaint category for Once-Only violations, separate from the general rights-request process.

- Give citizens the right to request confirmation that a PIA was completed for a specific system, mirroring the disclosure precedent for automated-decision systems (clause 14.5A).

- The redress framework should also provide for victim compensation where a breach or unlawful disclosure causes demonstrable harm, rather than stopping at corrective action against the public body. Kenya's Office of the Data Protection Commissioner has issued compensation orders as a routine part of its enforcement toolkit (184 compensation orders issued as of January 2026, alongside penalty and enforcement notices), and UK and Australian practice shows equivalent mechanisms operating against public and private bodies alike. We recommend that the Draft Policy's redress instrument include an explicit compensation-order power, not only corrective directions, modelled on Kenya's compensation-order mechanism.

- Formalised federal-provincial collaboration through a binding intergovernmental instrument rather than relying on voluntary adoption. The NGDC (clause 16.5(b)), which already includes provincial representation, is the appropriate forum to negotiate such an instrument, but its current role is advisory and coordinating only, as it has no power to bind a non-consenting province.

- Establish mutual recognition protocols specifying minimum data-quality and security standards a provincial dataset must meet to be recognised as authoritative federally, and vice versa.

- Add an explicit liability and correction-responsibility clause to the WASL National Data Exchange Specification for errors that propagate across the federal-provincial boundary.

- Build a dispute-resolution mechanism into the same instrument for conflicting federal-provincial datasets.

- Require mandatory independent third-party audit for public bodies handling Tier 1/high-impact data, with self-assessment plus periodic sampling retained for lower-tier bodies.
- Establish and implement incident response mechanisms and reports in case of violations or data breaches.
- Publish the NDMI's underlying methodology and scoring criteria, not only headline results to create greater transparency and build public trust.
- Make all monitoring frameworks and models developed under the Policy available for independent review by external Pakistani industry and academic experts, reinforcing the separation of functions recommendation raised above.
- Employ data architects and technical support teams to troubleshoot incoming problems with data governance and to offer technical support to citizens where needed
- Create capacity-building programs that give public officials proper training and give them opportunities to get relevant certifications in data governance.
- Establish independent and third-party-ruled oversight boards for data governance processes to check for rollout, implementation, and any violations that may occur.