Data Governance Policy 2026

GOVERNMENT OF PAKISTAN
Ministry of Information Technology & Telecommunication

June – 2026

TABLE OF CONTENTS

1 Scope

This Policy establishes the binding national direction for the governance of public-sector data in the Islamic Republic of Pakistan, across the lifecycle from collection, generation, and acquisition; through use, sharing, and re-use; to retention, preservation, and lawful disposal.

This Policy is the primary national instrument for data governance. It declares the principles of the State; sets policy positions on sovereignty, openness, sharing, privacy, citizen empowerment, cross-border transfer, emerging technologies, and the data economy; establishes the institutional framework for execution; and authorises the supporting instruments listed in Annex II.

This Policy applies to all federal public bodies and their contractors, processors, and partners, as set out in clause 7. The detailed operating model, control architecture, technical standards, and procedural requirements are set out in the supporting instruments referenced in this Policy and shall be read consistently with it.

This Policy does not govern personal data held outside the public sector, primary legislation, judicial proceedings, or matters falling within the specific national-security, defence, parliamentary, or judicial regimes, save where expressly provided.

2 References

The following documents are referenced normatively. For dated references, only the edition cited applies. For undated references, the latest edition applies.

- Constitution of the Islamic Republic of Pakistan, in particular Articles 14 and 19A
- Digital Nation Pakistan Act, 2025 (Act No. I of 2025)
- Right of Access to Information Act, 2017
- Electronic Transactions Ordinance, 2002
- Prevention of Electronic Crimes Act, 2016

3 Definitions

For the purposes of this Policy, the following terms shall bear the meanings set out below.

3.1 Agency CDO: the senior official designated by a public body to lead implementation of this Policy and supporting instruments within that body.

3.2 Authoritative source: the designated source of record for a defined data domain, data element, reference dataset, or master dataset.

3.3 Child: a natural person below the age of eighteen years, consistent with the Majority Act, 1875 (IX of 1875). Where a special law applicable to a particular matter prescribes a different age, the special law shall apply for that matter.

3.4 Conformance: demonstrated compliance with the mandatory requirements, profiles, controls, or specifications prescribed by this Policy or by PDA-issued supporting instruments.

3.5 Cross-border transfer: any movement of Government data, or any material remote accessibility to it, from within Pakistan to another jurisdiction, or by persons operating under another jurisdiction.

3.6 Data Sharing Impact Assessment (DSIA): a structured assessment of the lawful basis, proportionality, risks, safeguards, and benefits of a proposed inter-agency or third-party data exchange.

3.7 Data subject: an identified or identifiable natural person to whom personal data relates.

3.8 Government data: any data processed by, for, or on behalf of a public body in the discharge of public functions, including records, derived data, metadata, and operational or analytical data.

3.9 Granular consent: consent that is specific to individual purposes and individual data elements, freely given, informed, demonstrable, and withdrawable.

3.10 High-impact use: any processing, system, or data use whose failure, misuse, inaccuracy, or unauthorised disclosure may materially affect rights, services, security, public trust, or continuity of essential functions.

3.11 Lawful basis: the legal ground, authority, condition, or other recognised basis under applicable law that permits a public body to process personal data for a defined purpose.

3.12 Metadata: structured information that describes the identity, meaning, origin, ownership, quality, classification, restrictions, lifecycle status, or technical characteristics of data, datasets, interfaces, or records.

3.13 National Data Governance Council (NDGC): the apex national forum for coordination and harmonisation of data governance, established by PDA under clause 16.5.

3.14 National Data Exchange (WASL): WASL (وصل) — the governed national interoperability pathway for inter-agency data exchange, established under DNP-D.002 RA.

3.15 National Data Maturity Index (NDMI): the principal national outcome-measurement instrument for assessing data-governance maturity across public bodies, published by PDA.

3.16 Open data: Government data released for public use under lawful terms after appropriate eligibility, quality, security, and disclosure-risk controls have been applied.

3.17 Personal data: data relating to an identified or identifiable natural person, as defined under applicable law. Personal data is not "owned" by any public body; it is held under fiduciary duty as set out in this Policy.

3.18 Primary Data Register: an authoritative national dataset, designated under clause 6.4A, on which other public bodies are required to rely as the source of record for the data domain it covers.

3.19 Privacy-Enhancing Technologies (PETs): a class of technical methods designed to protect personal data and enable analysis or verification with minimal disclosure of underlying data.

3.20 Provenance: documented knowledge of a dataset's source, lineage, transformations, custody, and use context, sufficient to support trust, auditability, and evidentiary integrity.

3.21 Public body: any ministry, division, department, agency, authority, commission, statutory body, public-sector organisation, public-sector company, or other entity that performs public functions or controls Government data.

3.22 Residency: the jurisdictional location in which data is hosted, stored, processed, or made materially accessible.

3.23 Selective disclosure: a technique by which a holder of credentials or attributes discloses to a verifier only the specific attributes or claims required for a stated purpose.

3.24 Sensitive personal data: a category of personal data that requires enhanced protection because of the nature of the data and the harm that could arise from its misuse or disclosure.

3.25 Sovereign control: the governance, legal, technical, and operational conditions that ensure Government data remains subject to Pakistan's lawful authority, defined accountability, and effective control.

3.26 Supporting instrument: any framework, standard, profile, code of practice, guideline, regulation, or other instrument issued by PDA under this Policy.

3.27 Zero-knowledge proof: a cryptographic method by which one party demonstrates to another that a statement is true without disclosing any information beyond its validity.

4 Abbreviations

Abbreviation	Definition
ADM	Automated Decision-Making
AI	Artificial Intelligence
CDO	Chief Data Officer
DNP	Digital Nation Pakistan
DPI	Digital Public Infrastructure
DSIA	Data Sharing Impact Assessment
ETO	Electronic Transactions Ordinance, 2002
MoITT	Ministry of Information Technology and Telecommunication
NCDO	National Chief Data Officer
NDGC	National Data Governance Council
NDMI	National Data Maturity Index
NDS	National Data Strategy
PDA	Pakistan Digital Authority
PDPL	Personal Data Protection Law (anticipated)
PECA	Prevention of Electronic Crimes Act, 2016
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
RTI	Right of Access to Information Act, 2017
SRO	Statutory Regulatory Order
WASL	National Data Exchange

5 The National Data Doctrine

> *Government data is a strategic national asset of the Islamic Republic of Pakistan, held in trust for the people. It shall be governed for sovereignty, public value, citizen empowerment, and lawful use.*

5.1 The asset proposition

Government data — collected from the citizen, generated through public administration, derived from analysis, or produced by sensors and systems operated by the State — possesses national value across multiple dimensions: administrative, civic, economic, scientific, and strategic.

5.2 Trust, not ownership

Government data is not the property of the agency that holds it. Public bodies are custodians, not proprietors. Custodianship carries the duty of stewardship: to protect, to maintain quality, to make discoverable, to share lawfully, and to disclose proportionately. Personal data, in particular, is not the subject of any ownership claim by a public body; it is held under fiduciary duty to the data subject.

5.3 Public value as the test

The test of every act of data governance — collection, retention, sharing, restriction, disclosure, deletion — is whether it advances public value, consistent with the Constitution and applicable law. Where public value is not advanced, the act is not justified by inertia, by precedent, or by administrative convenience.

5.4 Sovereignty as the condition

Pakistan asserts sovereign control over Government data. Sovereignty is the condition under which the asset is governed. It is preserved by default and yielded only by specific authorisation, with safeguards.

5.5 Federation as the architecture

Pakistan is a federation. Custodianship of data follows the constitutional and legal allocation of public functions. National coherence is achieved not by centralisation but by federation: distributed custody, common standards, and governed exchange. Each public body owns, controls, and serves its own data; the State, acting through this Policy and its supporting instruments, ensures that the whole is coherent.

5.6 The citizen as the centre

The asset framing of this clause does not diminish the rights of the citizen; it is conditional upon them. The citizen is the active beneficiary of data governance, with rights of consent, access, correction, portability, and erasure. The substantive citizen-empowerment provisions are set out in clause 12.

6 Foundational principles

The following principles SHALL guide the interpretation and implementation of this Policy. They apply concurrently and shall be balanced against one another with regard to the Constitution and applicable statutes.

6.1 Data as national asset

Government data is held in trust for the people of Pakistan. Custodianship entails active stewardship of quality, metadata, security, accessibility, and lawful use.

6.2 Sovereignty by default

Government data shall remain under the lawful authority and effective control of Pakistan. Cross-border transfer is an exception requiring specific governance, justification, and safeguards.

6.3 Federation of custody

Operational custody remains with the public body that lawfully collects or generates the data. Each public body, federal or provincial, owns, controls, and serves its own data, governed under nationally consistent obligations and enabled through governed exchange. Personal data of the citizen shall not be duplicated, replicated, or centrally pooled save where expressly authorised under this Policy.

6.4 Authoritative source discipline

For every data domain or reference dataset of national importance, a single authoritative source shall be designated, and other systems shall consume from it. This principle is the foundation of inter-agency interoperability and is therefore a Policy-level commitment, with operational designation governed by the supporting instruments.

6.4A Primary Data Registers

Certain authoritative datasets are foundational to the operation of the State and the realisation of citizens' rights. These datasets, designated under this clause, shall be known as Primary Data Registers.

The list of Primary Data Registers shall be designated by the Federal Cabinet on the recommendation of PDA, after consultation through the National Data Governance Council and with the Provincial Governments where the relevant subject matter so requires. The list shall be elaborated in the National Data Strategy and may be amended from time to time through the same process.

For each Primary Data Register, PDA, on the recommendation of the relevant sector and in consultation with the National Data Governance Council, shall designate a custodian public body. The custodian is accountable for the currency, quality, integrity, security, and lawful accessibility of the register. Sectoral regulators, line ministries, and provincial counterparts shall support PDA in the identification, designation, curation, and maintenance of Primary Data Registers in their respective domains.

Public bodies shall consume from Primary Data Registers as the authoritative source for the data domain each register covers, and shall not maintain duplicate copies save where expressly authorised under this Policy or the supporting instruments.

NOTE — Primary Data Registers typically cover foundational entities and relationships such as natural persons, legal entities, addresses and places, immovable property, and vehicles. The specific designation of Pakistan's Primary Data Registers shall be made by the Federal Cabinet on the recommendation of PDA in accordance with this clause, and shall be elaborated in the National Data Strategy.

6.5 Open by default, closed by exception

Public-sector data shall be open by default, subject to lawful classification. Restrictions shall be applied by exception, on the narrowest grounds permitted by law, with reasons recorded and reviewable.

6.6 Once-only principle

The citizen shall not be required to provide the same information to the State more than once, unless such repetition is necessary by law or for verification.

6.7 Minimum disclosure

In every act of sharing or disclosure, only the minimum data necessary for the lawful purpose shall be exchanged. Field-level minimisation, aggregation, de-identification, and Privacy-Enhancing Technologies shall be applied where they meet the purpose.

6.8 Interoperability by standards

Data shall be maintained, exchanged, and published in standardised, machine-readable, non-proprietary formats. Conformance to PDA-issued interoperability profiles is mandatory for governed exchange.

6.9 Quality and provenance

Government data shall be accurate, complete, timely, consistent, and fit for purpose. Provenance and lineage shall be documented sufficiently to support trust, auditability, and evidentiary integrity.

6.10 Privacy by design

Privacy protections shall be embedded into the design of systems, processes, and data practices. Public bodies shall employ Privacy-Enhancing Technologies appropriate to the purpose, in accordance with the supporting instruments.

6.11 Citizen empowerment and informational self-determination

The citizen shall be empowered to know what data is held about them, to consent or refuse where consent is the lawful basis, to know who within Government has accessed their data, and to assert rights of correction, portability, and erasure.

6.12 Lawful basis

Personal data shall be processed only on a lawful basis recognised in applicable law. Purpose specification, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality apply to all processing of personal data.

6.13 Zero trust and continuous verification

Access to Government data shall be governed on zero-trust principles: identity- and policy-driven access decisions, least privilege, strong authentication, and continuous verification, monitoring, and audit.

6.14 Security proportionality

Security controls shall be proportionate to the classification, sensitivity, and exposure of the data and to the risk of harm from compromise.

6.15 Accountability and transparency

Public bodies shall be responsible for, and able to demonstrate compliance with, the principles and requirements of this Policy. Roles and decision rights shall be explicit, documented, and reviewable.

6.16 Public value and innovation

The governance of data shall maximise public value: better services, better policy, broader innovation, and economic growth, consistent with the protection of rights, security, and the public interest.

6.17 Continuous improvement

This Policy and its supporting instruments shall be subject to periodic review, evidence-based revision, and structured stakeholder engagement.

7 Scope of application

7.1 Application to federal public bodies

This Policy applies to all federal ministries, divisions, departments, attached departments, subordinate offices, statutory corporations, regulators, authorities, commissions, autonomous bodies, and public-sector companies under federal jurisdiction; to all entities receiving public funds for the management of data on behalf of the Federal Government; and to all contractors, processors, concessionaires, grantees, and partners that process Government data or perform public functions.

7.2 Provincial harmonisation

This Policy applies to federal public bodies. PDA shall coordinate with provincial governments — through the National Data Governance Council under clause 16.5 — to promote harmonisation of data-governance standards, mutual recognition of authoritative sources, and federation-aligned exchange. Provincial governments are encouraged to adopt this Policy or equivalent frameworks.

7.3 Flow-down obligations

All agreements involving Government data shall include enforceable obligations binding the counterparty to compliance with this Policy and the applicable supporting instruments. Non-compliance by a processor or contractor does not relieve the public body of its responsibilities under this Policy.

7.4 Lawful adaptations

The application of specific obligations may be modified, in coordination with PDA, to give effect to lawful national-security, defence, intelligence, parliamentary, or judicial considerations, in which cases an adapted regime, consistent with this Policy and applicable law, shall apply.

7.5 Extraterritorial reach

Where Government data is processed, stored, or accessed outside Pakistan, the obligations under this Policy follow the data.

8 Data sovereignty and residency

8.1 Position

The Government of Pakistan asserts sovereign control over Government data. Sovereignty is a function of legal authority, residency, technical control, and operational practice acting together.

8.2 Residency tiers

Residency obligations shall apply on a tiered basis as follows.

Tier	Applies to	Requirement
Tier 1 — Mandatory in-country residency	RESTRICTED, CONFIDENTIAL, and personal data, including all sensitive personal data and authoritative-source data of national importance	Hosted, stored, and processed within the territory of Pakistan. Cross-border processing or remote access requires specific PDA approval and additional safeguards.
Tier 2 — Approval-based offshore processing	INTERNAL data not within Tier 1, where a credible operational case exists for offshore processing	May be processed offshore with prior PDA approval, subject to contractual safeguards, technical controls, and audit and oversight rights.
Tier 3 — No residency restriction	OPEN data	May be hosted, mirrored, and re-used globally, subject to attribution and licence terms.

8.3 Sovereign control measures

For designated categories of data, PDA may require additional sovereign control measures, including jurisdictional safeguards on cryptographic key custody, to ensure that Government data remains subject to Pakistan's effective control. The detailed scheme is set out in the Sovereignty, Residency, and Cross-Border Controls Instrument.

8.4 Foreign-jurisdiction access

Where a court, regulator, or authority of a foreign jurisdiction requires the production of, or access to, Government data, the public body or processor in receipt of the request shall promptly notify PDA, shall not voluntarily disclose, and shall comply only as permitted by Pakistani law and applicable mutual legal assistance arrangements.

9 Open data

9.1 Position

Public-sector data is open by default. Data shall be made available for public use under lawful terms, in machine-readable formats, with metadata, and through the National Open Data Portal, except where lawful classification or specific statutory restriction applies.

9.2 Eligibility

Eligibility for open publication is determined through proportionate eligibility, quality, security, and disclosure-risk controls, in accordance with the Open Data and Controlled Access Instrument. Disclosure-risk assessment includes consideration of re-identification risk, mosaic effects, and cumulative-disclosure risk.

9.3 Licensing

All open data shall be released under the Pakistan Open Government Licence, or another licence approved by PDA, permitting unrestricted use, modification, and redistribution subject to attribution and other reasonable conditions.

9.4 Proactive disclosure

Public bodies shall maintain a published inventory of the datasets they hold, the classification of each, and the availability status, consistent with their proactive-disclosure obligations under the Right of Access to Information Act, 2017.

9.5 Citizen feedback and contestability

Public bodies shall provide accessible mechanisms for the public to query, correct, and contest published data. Where data is found to be inaccurate or misleading, the public body shall correct it without undue delay.

10 Data sharing and re-use

10.1 Position

Authorised data exchange between public bodies, and the lawful re-use of public-sector data by approved third parties, are essential to the realisation of public value from data.

10.2 Inter-agency exchange through WASL

Inter-agency data exchange shall be conducted through WASL (وصل), the National Data Exchange, in accordance with the National Data Exchange and Interoperability Instrument and the Reference Architecture set out in DNP-D.002 RA. Public bodies shall not establish ad hoc data-sharing arrangements outside the governed exchange except as expressly authorised by PDA.

10.3 Lawful basis for sharing

All inter-agency exchange shall be supported by a lawful basis, a registered purpose, an approved interoperability profile, and clear conditions of use, with the conditions of use flowing with the data through the exchange.

10.4 Data Sharing Impact Assessment

Cross-agency or third-party data exchanges, particularly those involving personal data, large-scale datasets, sensitive sectors, or new sharing patterns, shall be subject to a Data Sharing Impact Assessment in accordance with the Privacy by Design and Impact Assessment Instrument.

10.5 Privacy-Enhancing Technologies in exchange

Where exchange involves personal or sensitive non-personal data, public bodies shall apply Privacy-Enhancing Technologies, where technically feasible and purpose-appropriate, to minimise the disclosure of underlying data while meeting the lawful purpose. The applicable techniques are specified in the Data Security Standards Instrument.

10.6 Controlled access for re-use

Purpose-bound, permissioned access to non-open Government data may be granted to approved researchers, innovators, and other lawful re-users, in accordance with the Open Data and Controlled Access Instrument. Conditions for re-use shall be non-discriminatory, transparent, proportionate, and objectively justified.

10.7 Once-only operationalisation

PDA shall designate priority once-only data flows in the National Data Strategy. Public bodies shall progressively adopt the once-only flows as prescribed.

11 Personal data and privacy

11.1 Position

The processing of personal data by public bodies shall be lawful, fair, transparent, and respectful of the constitutional right to privacy under Article 14 of the Constitution.

11.2 Lawful basis

Personal data shall be processed only on a lawful basis recognised in applicable law, including consent, contract, legal obligation, vital interests, or the performance of a public task.

11.3 Data subject rights

Data subject rights shall be recognised and given effect as provided by applicable law and as elaborated in the Privacy by Design and Impact Assessment Instrument and the Rights Handling, Notices, and Redress Instrument. Where the Personal Data Protection Law is enacted, this Policy shall be updated to align with the statutory regime. The substantive citizen-empowerment provisions are set out in clause 12.

In respect of personal data, this Policy shall be read consistently with applicable personal data protection law. Where such law confers rights or imposes obligations more protective of the data subject than this Policy, the more protective provision shall apply.

11.4 Privacy Impact Assessment

High-impact processing — including processing involving sensitive personal data, large-scale processing, profiling and automated decision-making with legal or similarly significant effects,

the deployment of new technologies, and the integration or large-scale linkage of datasets — shall be subject to a Privacy Impact Assessment.

11.5 Sensitive personal data

Sensitive personal data shall be subject to enhanced safeguards, including stricter access controls, mandatory encryption, narrower retention, explicit lawful basis, and heightened audit.

11.6 Children's data

The processing of data relating to children, as defined in clause 3.3, shall be subject to enhanced protections, including specific lawful basis, age-appropriate notice, restrictions on profiling and behavioural advertising, and parental or guardian engagement where required.

11.7 Notices and redress

Public bodies shall provide accessible privacy notices, intake channels for rights requests, defined response timelines, and complaint-handling pathways. Redress shall be effective, accessible, and free of charge except where a request is manifestly unfounded or excessive.

11.8 Breach notification

Public bodies shall notify PDA of personal data breaches without undue delay and within the timelines prescribed in the Compliance, Audit, and Certification Instrument. Where a breach is likely to result in a high risk to the rights and freedoms of natural persons, the affected individuals shall also be notified.

Where a breach involves personal data, public bodies shall additionally notify the authority designated under the personal data protection law, in accordance with the timelines and procedures prescribed by that law. PDA and the authority designated under the personal data protection law shall coordinate to ensure consistency of breach response and to avoid duplicative obligations on public bodies.

11.9 Storage limitation and retention by default

Every processing of personal data shall have a defined retention period, proportionate to the lawful purpose for which the data is held. Personal data shall not be retained beyond the defined period save where expressly required by applicable law or by judicial process. Public bodies shall maintain documented retention schedules and shall securely dispose of personal data at the end of the retention period in accordance with the Preservation, Retention, and Disposal Standard.

12 Citizen data rights and empowerment

> *The citizen is not a passive subject of data governance but its active beneficiary. The Government of Pakistan recognises and shall give effect to the rights, agency, and empowerment of the citizen in the governance of data held about them.*

12.1 Position

Informational privacy and citizen empowerment are not merely safeguards against State action; they are the foundation of public trust. The citizen has rights over data held about them by the State, and the State shall provide the technical and procedural means by which those rights can be meaningfully exercised.

12.2 Granular consent

Where consent is the lawful basis for processing, it shall be granular, specific, informed, demonstrable, and withdrawable. The State shall not rely on bundled or take-it-or-leave-it consent for the processing of personal data. The technical and procedural standards for consent are set out in the Privacy by Design and Impact Assessment Instrument and the Rights Handling, Notices, and Redress Instrument.

12.3 Access transparency

Every citizen shall have the right, on request, to know who within Government has accessed their personal data, when, and for what purpose. This right shall not be denied except on narrow grounds expressly provided by law, with reasons recorded.

12.4 Privacy-Enhancing Technologies

Public bodies shall, in the design and operation of systems that process personal data, employ Privacy-Enhancing Technologies appropriate to the purpose. The applicable techniques and adoption profiles are set out in the Data Security Standards Instrument and the Privacy by Design and Impact Assessment Instrument.

12.5 Selective disclosure and zero-knowledge verification

Where an attribute, claim, or eligibility about the citizen can be verified through cryptographic techniques that do not require disclosure of the underlying data — including zero-knowledge proofs and selective-disclosure credentials — public bodies shall not require disclosure of the underlying data. The technical schemes are specified in the Citizen Identity and Credentials Instrument.

12.6 Data portability and citizen-held credentials

The citizen shall have the right to obtain personal data held about them in a structured, commonly used, and machine-readable format, and to have such data transmitted directly between public bodies where technically feasible and lawful. PDA shall enable a national scheme of citizen-held verifiable credentials, with the technical and governance framework set out in the Citizen Identity and Credentials Instrument.

12.7 Right to rectification and erasure

The citizen shall have the right to obtain rectification of inaccurate or incomplete data, and the right to obtain erasure of personal data, subject to lawful exceptions including the requirements of public records, judicial proceedings, statutory retention, and the exercise of constitutional functions.

12.8 Federated custody reinforced

Personal data of the citizen shall remain with the public body lawfully responsible for it. Access by other public bodies, where lawful and necessary, shall be through governed exchange

under clause 10, and not through duplication, replication, or central pooling, save where expressly authorised under this Policy.

12.9 Right to meaningful human review

Where decisions affecting the citizen with legal or similarly significant effects are taken by automated means, the citizen shall have the right to request meaningful human review, in accordance with clause 14 and the AI, ADM, Emerging Technology, and Spatial Governance Instrument.

13 Cross-border data transfer

13.1 Position

Cross-border transfer of Government data is permitted only where it is lawful, justified, governed, and safeguarded, and where the sovereign control of Pakistan over the data is not compromised.

13.2 Approval pathways

Cross-border transfer shall be authorised through approval pathways differentiated by data classification, sensitivity, intended use, and recipient jurisdiction, as set out in the Sovereignty, Residency, and Cross-Border Controls Instrument.

13.3 Adequacy

PDA may, by notification, recognise jurisdictions that provide an adequate level of protection for transferred data. In the absence of an adequacy determination, transfer shall be subject to approved standard contractual clauses, binding institutional rules, certifications, or other safeguards approved by PDA.

13.4 Public emergencies and public-interest cooperation

Lawful international cooperation in response to public emergencies, cross-border crime, public-health events, environmental risk, or other compelling public interest shall be facilitated under defined safeguards, with notification to PDA and proportionate handling of personal data.

13.5 Onward transfer

Conditions on cross-border transfer shall extend to onward transfers, with equivalent protections required at each subsequent stage.

13.6 Personal data in cross-border transfer

Where personal data is involved in a cross-border transfer of Government data, the transfer is subject to both this Policy and any applicable personal data protection law. Where the two regimes prescribe different requirements, the more protective requirement shall apply.

14 Artificial intelligence and emerging technology

14.1 Position

The Government of Pakistan shall harness artificial intelligence, automated decision-making, and emerging data-intensive technologies for public value, while protecting rights, ensuring lawful use, and preserving meaningful human oversight where required.

14.2 Risk-tiered controls

Uses of AI and ADM shall be governed under a risk-tiered approach. High-risk uses, including those with legal or similarly significant effects on individuals, shall be subject to higher-rigor controls including pre-production registration, model accountability, explainability commensurate with use, drift monitoring, and post-deployment review.

14.3 Data foundations for AI

The use of Government data for the training, fine-tuning, validation, or operation of AI systems shall be governed under this Policy, including obligations relating to lawful basis, classification, provenance, quality, residency, and the application of Privacy-Enhancing Technologies. PDA shall promote an AI-ready data programme to enable safe and effective AI use across the public sector.

14.4 Human oversight

Automated decisions with legal or similarly significant effects shall provide for meaningful human review on request, transparent contestability, and accessible redress. Human oversight shall be substantive and not merely formal.

14.5 Procurement and assurance

Procurement of AI and emerging-technology systems by public bodies shall include data-governance, security, and ethics requirements aligned with this Policy and the relevant supporting instruments.

14.5 A Algorithmic transparency

Public bodies operating automated decision systems with legal or similarly significant effects on individuals shall publish, in a public registry maintained by PDA, a description of each such system, including its purpose, the categories of data inputs used, and the decision logic at a level of abstraction appropriate to security, intellectual property, and operational integrity. Detailed requirements are set out in the AI, ADM, Emerging Technology, and Spatial Governance Instrument.

14.6 Generative AI

The use of generative AI by public bodies, including for the production of content, decisions, or analyses that materially affect citizens, shall be subject to specific controls relating to provenance disclosure, factual accuracy, intellectual-property compliance, and data leakage.

14.7 Geospatial and sensor data

Geospatial, Internet-of-Things, and sensor data shall be governed consistently with this Policy, with specific profiles where required, recognising the particular sensitivities and value of these data types.

15 Data value and the data economy

> *The Government of Pakistan recognises that public-sector data, governed responsibly, is not only an instrument of administration but an enabler of national prosperity, scientific progress, and citizen-centred innovation.*

15.1 Position

Government data, beyond its administrative use, has the capacity to generate economic, scientific, and social value when shared lawfully and responsibly. The Government shall enable, and where appropriate actively promote, the realisation of that value, consistent with the rights of data subjects, the protection of national interests, and the principles of this Policy. The pursuit of value is conditional, in every case, upon the safeguards set out in clauses 11 and 12.

15.2 Public-private data partnerships

PDA may authorise structured partnerships between public bodies and private-sector, academic, civil-society, or international entities, for purposes including research, innovation, service co-creation, and the development of public-interest data products. Such partnerships shall be governed by clear lawful basis, defined safeguards, and the application of Privacy-Enhancing Technologies where relevant.

15.3 Data trusts and data intermediaries

PDA may recognise, register, and supervise data trusts and data intermediaries where such arrangements support the lawful pooling, sharing, or stewardship of data for the public good. Recognition shall be subject to fiduciary, security, and conformance requirements established by PDA in the Data Value and Re-Use Instrument.

15.4 Licensing and value capture

Where public-sector non-personal data is made available for re-use under terms other than the standard open licence, PDA may prescribe licensing models, pricing principles, attribution requirements, and value-capture mechanisms. Pricing and licensing shall not unduly restrict competition or innovation, and shall not compromise the rights of data subjects or the public interest.

15.5 Safe-harbour for non-personal data sharing

To encourage responsible non-personal data sharing for innovation and public benefit, PDA may, by instrument, establish safe-harbour arrangements specifying the conditions under which approved sharing of non-personal data shall be deemed compliant with this Policy.

15.6 Data altruism

Individuals and organisations may contribute personal or non-personal data, on a voluntary and informed basis, for objectives of public interest, through arrangements recognised by

PDA. Recognised data-altruism arrangements shall provide for explicit, informed, granular consent; transparency; beneficiary rights; and effective oversight.

15.7 Citizen consent paramount

No arrangement under this clause shall override the citizen-empowerment provisions set out in clause 12. Where personal data is involved, granular consent, access transparency, and the application of Privacy-Enhancing Technologies are non-negotiable conditions of value-creation.

15.8 Sovereign value preservation

The realisation of value from public-sector data shall not compromise sovereign control over authoritative-source data of national importance, nor shall it permit the transfer of effective control over such data to entities operating under foreign jurisdiction.

15.9 Equity and inclusion

In all arrangements under this clause, PDA shall have regard to equitable access, non-discrimination, and the inclusion of small and medium enterprises, academic institutions, and civil-society actors, including those operating in underserved regions of Pakistan.

16 Institutional framework

16.1 Pakistan Digital Authority

PDA is the national authority responsible for the issuance, oversight, and assurance of this Policy and its supporting instruments, in exercise of its powers under the Digital Nation Pakistan Act, 2025. PDA's functions include the issuance of supporting instruments listed in Annex II; stewardship of the National Data Catalogue; oversight of WASL; the National Open Data Portal; compliance, conformance, audit, and corrective action; recognition and supervision of data trusts and intermediaries; capacity-building; and periodic public reporting.

16.2 Directions

PDA may issue binding directions to public bodies for the purpose of giving effect to this Policy and its supporting instruments. Directions shall be in writing, with reasons, and shall provide a reasonable opportunity for representation by the public body concerned.

16.3 National Chief Data Officer

Pakistan Digital Authority shall designate a National Chief Data Officer to drive cross-government execution of this Policy; sequence implementation; coordinate Agency CDOs and provincial counterparts; maintain the national-level dashboard of compliance, conformance, and the National Data Maturity Index; and report to PDA leadership and the National Data Governance Council.

The National Chief Data Officer reports to Pakistan Digital Authority, and exercises authority under this Policy and the supporting instruments. The role is operational and executive.

16.4 Agency Chief Data Officers

Each public body within scope of this Policy shall designate an Agency Chief Data Officer of appropriate seniority and competence. The Agency CDO shall lead implementation within the

public body, maintain inventory and metadata, ensure quality and lawful use, respond to data-subject requests, report incidents, and submit periodic compliance reports. Public bodies shall position the Agency CDO with sufficient authority, access, budget, and direct reporting line to the head of the public body.

16.5 National Data Governance Council

PDA shall, by notification, establish a National Data Governance Council as the apex national forum for coordination and harmonisation of data governance.

The Council shall be chaired by the Pakistan Digital Authority, and shall comprise representatives drawn from the following categories:

(a) the Federal Government, including the Ministry responsible for information technology and telecommunications;

(b) the Provincial Governments;

(c) sectoral regulators with material data-governance interests, including those responsible for finance, telecommunications, securities, identity, and other critical sectoral domains;

(d) federal authorities with custodianship of Primary Data Registers;

(e) the National Chief Data Officer; and

(f) such other public, private, academic, or civil-society members as PDA may designate from time to time, having regard to the matters under consideration.

The Council shall consider strategic priorities and sequencing under this Policy and the National Data Strategy; promote federation-aligned exchange and the mutual recognition of authoritative sources; advise on the designation, custodianship, and curation of Primary Data Registers; review the National Data Maturity Index and consider corrective measures; and consider such other matters as PDA may refer to it.

The composition, secretariat arrangements, decision-making procedures, quorum, and operating rules of the Council shall be determined by PDA and elaborated in the National Data Governance Framework. PDA shall ensure that the Council's composition reflects the federal, provincial, sectoral, and citizen interests in data governance.

16.6 Sectoral coordination

PDA shall coordinate with sectoral regulators where domain-specific data regimes apply, and shall conclude memoranda of understanding where required to clarify boundaries, harmonise standards, and avoid duplication.

16.7 Provincial coordination

PDA shall coordinate with provincial governments, primarily through the National Data Governance Council, to promote a federated, harmonised national data ecosystem.

16.8 International cooperation

PDA may engage with international counterparts, multilateral bodies, and standards organisations to advance Pakistan's interests in cross-border data governance, mutual recognition, and the responsible international flow of data.

16.9 Coordination with the personal data protection authority

PDA's mandate under this Policy is the governance of public-sector data as a national asset, including the operating arrangements, standards, and supporting instruments by which public bodies collect, process, share, and dispose of Government data. 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.

PDA and the authority designated under the personal data protection law shall coordinate through a memorandum of understanding to ensure consistency, avoid duplicative directions on public bodies, share supervisory information where lawful, and respect each other's jurisdiction. Where the two authorities issue directions or guidance on the same subject, those directions shall be reconciled through consultation and, where necessary, joint instruments.

17 Implementation

17.1 Instrument hierarchy

This Policy is the primary national instrument for data governance. Below this Policy, PDA shall issue and maintain the National Data Governance Framework; standards and profiles; procedures, codes of practice, and guidance; the National Data Strategy; and such further instruments as PDA considers necessary. In the event of any inconsistency between this Policy and a supporting instrument, this Policy prevails.

17.2 National Data Strategy

PDA shall publish, and periodically revise, the National Data Strategy, which shall set out priority datasets and services for sequenced implementation; priority once-only data flows; priority sectoral pathways; capability and capacity-building milestones; and assurance and outcomes measurement, anchored in the National Data Maturity Index.

17.3 Sequenced implementation

The implementation of this Policy shall proceed in a sequenced manner consistent with the capacity of public bodies, the maturity of supporting instruments, and the priorities set in the National Data Strategy. PDA shall publish indicative implementation timelines and shall track and report progress.

17.4 Public register of instruments

PDA shall publish, and maintain, a public register of all live supporting instruments, with version, status, effective date, and brief description, on the Standards Portal at https://standards.dnp.gov.pk.

18 Compliance, conformance, and maturity

18.1 Compliance

Public bodies shall comply with this Policy and the applicable supporting instruments. Compliance shall be evidenced through reporting, conformance assessments, audits, and certifications as prescribed.

18.2 Conformance

Conformance with prescribed standards, profiles, and controls shall be demonstrated through tests, certifications, and other arrangements as prescribed in the Compliance, Audit, Certification, and Maturity Instrument. Conformance is the technical companion to compliance and is necessary for participation in WASL and other governed pathways.

18.3 National Data Maturity Index

PDA shall establish, maintain, and publish the National Data Maturity Index as the principal national instrument for measuring data-governance maturity across public bodies. The NDMI shall assess governance, quality, security, sharing, openness, citizen-empowerment, and capability dimensions. NDMI results shall be published annually and shall inform corrective action, prioritisation, and recognition.

18.4 Reporting and audit

Agency CDOs shall report periodically to PDA on data-governance status, incidents, NDMI inputs, and corrective actions. PDA shall conduct, or commission, periodic audits of public bodies' compliance with this Policy and the supporting instruments. Audit reports, with appropriate redactions, may be published in support of accountability.

18.5 Corrective action and enforcement

Where non-compliance is identified, PDA shall require corrective action through binding directions, with timelines and follow-up assurance. Persistent or material non-compliance shall be addressed through the enforcement mechanisms set out in the Compliance, Audit, Certification, and Maturity Instrument and applicable law.

18.6 Review

This Policy shall be reviewed by PDA not less than once every three years, and earlier where required by significant changes in the legal, technological, or institutional landscape. Material amendments shall be subject to public consultation, save where urgency requires otherwise.

19 Conformity assessment

Conformity with this Policy is assessed as follows:

(a) annual self-assessment by every public body, signed by the Agency CDO and submitted to PDA in the form prescribed by the National Data Maturity Index;

(b) periodic third-party audit, commissioned by PDA, of a sample of public bodies and of any public body where material non-compliance is suspected;

(c) certification of conformance to specific supporting instruments, where the instrument provides for certification, in accordance with the Compliance, Audit, Certification, and Maturity Instrument; and

(d) public reporting by PDA of compliance status, NDMI results, and corrective actions, on the Standards Portal at https://standards.dnp.gov.pk.

Annex I (Normative) — Constitutional and Statutory Anchors

This Policy is grounded in:

I.1 the Constitution of the Islamic Republic of Pakistan;

I.2 the Right of Access to Information Act, 2017;

I.3 the Electronic Transactions Ordinance, 2002;

I.4 the Prevention of Electronic Crimes Act, 2016; and

I.5 the Digital Nation Pakistan Act, 2025.

This Policy is to be read consistently with future legislation enacted in the field of data, digital, and emerging-technology governance — including, in particular, any Personal Data Protection Law and any future statute on data governance and exchange and shall be revised, where required, to maintain consistency with such legislation.

Annex II (Normative) — Supporting Instruments

Without limiting the lawful discretion of PDA to issue further instruments, the following minimum supporting instruments shall be issued, or maintained, to give full operational effect to this Policy. Each instrument shall be issued under a distinct DNP-D series reference and shall be made available on the Standards Portal.

Reference	Instrument	Purpose
DNP-D.001 FWK	National Data Governance Framework	Detailed operating model, governance controls, lifecycle discipline, implementation requirements, assurance expectations. Establishes National Data Governance Council operating arrangements.
DNP-D.100 STD	Data Classification and Handling Standard	Classification levels, mandatory marking, handling, access, transmission, exception, break-glass, and disposal controls.
DNP-D.101 STD	Metadata and National Catalogue Standard	Mandatory metadata, catalogue requirements, stewardship obligations, and discoverability rules.
DNP-D.102 STD	Data Quality and Standardisation Standard	Data quality dimensions, rules, remediation, common data elements, authoritative-source discipline, master/reference data.
DNP-D.103 STD	Data Security Standards	Technical security controls (encryption, key management, access governance, zero-trust enforcement, logging, monitoring) proportionate to classification, including PET adoption profiles.
DNP-D.300 TS	WASL National Data Exchange Specification	Schemas, exchange profiles, trust, security, service management, and conformance for inter-agency exchange through WASL.
DNP-D.200 GDL	Open Data and Controlled Access Guideline	Publication eligibility, safe-release controls, controlled-access pathways, output restrictions, public feedback, correction, and dispute-handling.

Reference	Instrument	Purpose
DNP-D.050 REG	Pakistan Open Government Licence	Standard licence under which open data is released for public use, modification, and redistribution.
DNP-D.400 PRF	Sovereignty, Residency, and Cross-Border Controls Profile	Residency tiers, hosting conditions, cross-border approvals, sovereign control measures, and jurisdictional safeguards.
DNP-D.104 STD	Privacy by Design and Impact Assessment Standard	Privacy-by-design requirements, PIA and DSIA triggers and methods, granular consent standards, sensitive-data and children's-data protections.
DNP-D.105 STD	Citizen Identity and Credentials Standard	Verifiable credentials, identity wallets, zero-knowledge proofs, selective disclosure, citizen-held credential schemes.
DNP-D.401 PRF	AI, ADM, Emerging Technology, and Spatial Governance Profile	Higher-rigor controls for AI data use, model accountability, explainability, drift, pre-production registration, generative AI, spatial technologies.
DNP-D.201 GDL	Data Value and Re-Use Guideline	Public-private data partnerships, data trusts and intermediaries, licensing and value capture, safe-harbour, data altruism, equity provisions.
DNP-D.106 STD	Preservation, Retention, and Disposal Standard	Retention, archival transfer, preservation metadata, integrity checking, secure sanitisation.
DNP-D.107 STD	Compliance, Audit, Certification, and Maturity Standard	Evidence requirements, reporting, assurance lines, audits, testing, certifications, NDMI, deviation governance, corrective action.
DNP-D.108 STD	Rights Handling, Notices, and Redress Standard	Intake channels, identity proofing, response timelines, complaint handling, accessibility, access-log requests.
DNP-D.202 GDL	Training and Capacity-Building Guideline	Role-based competencies, minimum training expectations, proficiency targets, awareness obligations.
DNP-D.002 RA	WASL National Data Exchange Reference Architecture	Architectural model for WASL.
DNP-D.100 STR	National Data Strategy	National priorities, sequencing, priority datasets and services, sectoral pathways, capability and assurance milestones.

Annex III (Normative) — Effective Date and Transitional Provisions

III.1 Effective date

This Policy shall come into effect on the date of its formal issuance by PDA, following Cabinet approval and Gazette notification.

III.2 Transitional provisions

Public bodies shall bring their existing data, processes, contracts, and systems into conformity with this Policy in accordance with the timelines set out in the National Data Strategy and the relevant supporting instruments. Where conformity cannot be achieved within the prescribed timelines, the public body shall apply to PDA for a deviation, with a documented plan and risk acceptance.

III.3 Continuity of prior actions

Anything done, or any action lawfully taken, under existing data-related policies, frameworks, or arrangements shall, to the extent consistent with this Policy, continue to have effect until superseded by an instrument issued under this Policy.

III.4 Existing contracts

Contracts for data processing entered into before the effective date shall be reviewed and amended, where necessary, to incorporate the requirements of this Policy and applicable supporting instruments at the earliest contractual opportunity, and in any event within twelve months of the effective date or such longer period as PDA may approve.

III.5 Review

This Policy shall be reviewed not less than once every three years, and earlier where required by significant change in the legal, technological, or institutional landscape.

Bibliography

The following resources informed the development of this Policy. They are not normative references.

b-1 OECD (2014), Recommendation of the Council on Digital Government Strategies, OECD/LEGAL/0406.

b-2 OECD (2021), Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463.

b-3 Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance (Data Governance Act).

b-4 Regulation (EU) 2016/679 (General Data Protection Regulation).

b-5 Singapore, Public Sector (Governance) Act 2018.

b-6 United Arab Emirates, TDRA Smart Data Framework.

b-7 Saudi Arabia, National Data Management and Personal Data Protection Standards (SDAIA / NDMO).

b-8 Estonia, X-Road federated data exchange operating model.

b-9 India, DigiLocker and Aadhaar-enabled service stack.

b-10 ISO/IEC 38505-1:2017, Information technology — Governance of IT — Governance of data.

Machine-readable metadata

The following JSON-LD metadata block accompanies this Policy in accordance with clause 13 and Annex A.6 of DNP-X.001 FWK.


```
{   "@context": "https://standards.dnp.gov.pk/schema/dnp",    "identifier": "DNP-D.001 POL",   "publishingAuthority": {     "code": "PDA",     "name": "Pakistan Digital Authority"}, "title":  "National  Data  Governance  Policy",  "titleUrdu": "قومی ڈیٹا گورننس پالیسی",   "series": "D",   "type": "POL",  "status": "FD",   "maturityLevel": "PROPOSED",   "classification": "PUBLIC",  "version": "1.1",   "normativeReferences": [     "Constitution of the Islamic Republic of Pakistan (Articles 14, 19A)",     "Digital Nation Pakistan Act, 2025",  "DNP-X.001 FWK",     "DNP-D.002 RA"   ],   "dateApproved": "2026-05-XX",  "dateEffective": "[Upon Gazette notification]",   "dateReview": "2029-05",  "jurisdiction": "PK",   "gazetteReference": "[Pending Cabinet approval and SRO assignment]",   "persistentURL": "https://standards.dnp.gov.pk/DNP-D.001",   "urn": "[pending]",   "doi": "[pending]" }
```


— END OF PUBLICATION —