Digital Nation Pakistan

PAKISTAN DIGITAL AUTHORITY

Standards & Regulatory Publications — D-Series: Data Governance, Management & Exchange

DNP-D.250 GDL

WASL — Pakistan National Data Exchange Layer: Consent Guideline

Summary

This Guideline sets out recommended practice for obtaining, recording, enforcing, and revoking citizen consent for the exchange of personal data through WASL, Pakistan's National Data Exchange Layer. It supports the consent obligations of the Pakistan Digital Authority (WASL Participation) Regulations, 2026 (DNP-D.050 REG) and the consent framework defined in DNP-D.300 TS. In summary, this Guideline recommends that:

- consent be treated as a blocking precondition to any exchange of personal data, satisfying the validity tests of Section 4;
- each consent be evidenced by a purpose-bound, time-bound, and field-scoped consent artefact, and enforced at runtime;
- purpose limitation be observed, with no secondary use beyond the authorised purpose;
- citizens be able to revoke consent at any time, with immediate effect for future transactions; and
- AI systems acting as Consumers remain subject to the same consent model, and neither grant nor exercise consent on a citizen's behalf.

Document reference	DNP-D.250 GDL
Document type	Guideline (GDL)
Status / Version	Draft for Standards Board consideration — v0.1
Classification	PUBLIC
Issued under	Digital Nation Pakistan Act, 2025; DNP-D.050 REG
Read with	DNP-D.002 RA (Reference Architecture); DNP-D.300 TS (Technical Specification)

Note — This document is a Guideline (GDL) under DNP-X.001. In accordance with DNP-X.001 §7.1, it uses "should" to denote recommended practice. Mandatory consent obligations continue to arise under the Pakistan Digital Authority (WASL Participation) Regulations, 2026 (DNP-D.050 REG); this Guideline sets out recommended means of meeting them and does not itself create binding obligations.

1. Purpose and Legal Basis

1.1 This Guideline is issued by the Pakistan Digital Authority ("PDA" or "the Authority") in exercise of its powers under the Digital Nation Pakistan Act, 2025, and in support of the Pakistan Digital Authority (WASL Participation) Regulations, 2026 (DNP-D.050 REG) ("the Regulations"). It provides recommended practice for the WASL Consent Governance referenced in Section 10 of DNP-D.300 TS ("the Technical Specification") and recommends how to give effect to the consent obligations of the Regulations and the consent framework defined in DNP-D.002 RA ("the Reference Architecture"). This Guideline is advisory; the binding legal instrument remains the Regulations.

1.2 This Guideline is subordinate to the Act and to the Regulations. In the event of any inconsistency, the Act prevails over the Regulations, and the Regulations prevail over this Guideline. Terms defined in the Regulations, the Reference Architecture, or the Technical Specification bear the same meaning in this Guideline.

2. Scope and Application

2.1 This Guideline applies to every Participating Entity, to NADRA in its capacity as Platform Operator, to Delegated Channel applications and their sponsoring entities, and to any AI system invoking WASL APIs as a Consumer. It governs every exchange of personal data relating to a citizen conducted through WASL.

2.2 This Guideline does not govern data classified as Public (Tier 1) or Internal (Tier 2) under Section 11 of the Technical Specification, save that where any such dataset contains fields constituting personal data, the consent requirements of this Guideline apply to those fields at field level, as expressed in the applicable Consent Policy Record.

3. Consent as a Recommended Blocking Precondition

3.1 No personal data relating to a citizen should be accessed, requested, received, or exchanged through WASL unless the citizen has provided explicit, valid, and binding consent in accordance with the Regulations and this Guideline, or where a consent exemption approved under Section 8 of this Guideline applies.

3.2 Consent should be treated as a blocking precondition, not an optional or deferrable control. A getData request for a consent-governed dataset should remain pending until a valid consent artefact is obtained, and should be terminated with the error CONSENT_REQUIRED upon citizen rejection or timeout (Technical Specification Section 10).

3.3 No component of the Central WASL Platform, no Participating Entity, and no AI system may grant, presume, infer, or bootstrap consent on a citizen's behalf. Acceptance of general terms and conditions should not constitute consent.

4. Standards of Valid Consent

4.1 Consent is valid only where it is:

(a) freely given: not made a condition of access to an essential service, except where access to WASL verification is itself the service being rendered;

(b) specific: tied to a defined data domain, a defined Consumer, and a defined purpose drawn from the WASL Purpose Code Registry;

(c) informed: the citizen having been clearly informed, in plain language, of the identity of the Consumer, the specific data fields to be shared, the purpose of sharing, the duration of the consent, and the right to revoke;

(d) unambiguous: given through a clear affirmative action of the citizen; and

(e) revocable: capable of being withdrawn at any time through a PDA-approved consent management channel, with immediate effect for future transactions.

4.2 Consent requests and notifications should be presented in English, Urdu and applicable regional languages, in plain, non-technical language. Where AI-generated plain-language summaries are provided under Section 12.1.1 of the Reference Architecture, such summaries are accessibility aids governed under the DNP-A series; the signed consent artefact remains the sole legally binding record of the consent.

4.3 Consent should be collected through PDA-approved channels onbeing primarily the national PAK-ID application, and, as enabled, SMS/USSD, assisted consent at service delivery points, and call-centre support, so that citizens without smartphone access are not excluded (Reference Architecture Section 9.4).

5. Consent Artefacts

5.1 Every approved consent should be evidenced by a consent artefact conforming to the schema at Section 10.2 of the Technical Specification: a cryptographically signed, machine-verifiable record identifying the consent, the data subject, the Consumer, the Provider, the dataset and field scope, the declared purpose, the validity window, the collection channel, and carrying the citizen's PAK-ID signature (where applicable) and the WASL platform signature.

5.2 Consent artefacts should be purpose-bound, time-bound, and field-scoped. The validity period should not exceed the maximum permitted by the applicable Consent Policy Record and in no case three hundred and sixty-five (365) days without renewal by the citizen.

5.3 All consent actions, grant, renewal, rejection, expiry, and revocation, should be cryptographically recorded, time-stamped, and maintained in the Transaction Proof Layer (TPL) as immutable consent artefact references. The TPL records proofs and hashes only and should not record the content of the data exchanged.

6. Runtime Enforcement

6.1 Before any getDat request for a consent-governed dataset proceeds, the consent validations prescribed at Section 10.3 of the Technical Specification should be performed in sequence, including verification of the artefact's presence, platform signature, consent–request identity match, Consumer, Provider, dataset and purpose match, validity window, ACTIVE status, and field scope. Failure of any validation should result in denial of the request with the corresponding error code.

6.2 Enforcement is layered: the API Gateway, the Consent Layer, and the Provider's Fulfilment Layer should each independently enforce the applicable Consent Policy Record. No custom API, GraphQL endpoint, Delegated Channel, or event subscription provides a mechanism to bypass consent enforcement.

6.3 Event subscriptions to personal data are consent-bound: they should be established only under a valid consent artefact and should terminate automatically upon revocation or expiry of the underlying consent.

7. Purpose Limitation and Prohibition of Secondary Use

7.1 A Consumer should access data through WASL only for purposes expressly authorised in its Participation Agreement and consistent with the consent obtained from the data subject. Data received through WASL should not be used for any secondary purpose, including re-sharing, sale, profiling, or any purpose not stated to the data subject at the time of consent.

7.2 The purpose declared in every request envelope should match the purpose recorded in the consent artefact; a mismatch should cause the request to be rejected with the corresponding error code.

8. Exemptions from Consent

8.1 The requirement for citizen consent may be exempted only where the disclosure of personal data through WASL is: (a) mandated by or under any applicable law; (b) necessary for national security, the maintenance of public order, or public safety; (c) required for the prevention, detection, investigation, or prosecution of a criminal offence; (d) required for or in connection with legal proceedings before a court or tribunal; or (e) for the administration of justice under the order of a court of competent jurisdiction.

8.2 No exemption should have effect unless it has been subject to prior review and written approval by PDA, which should assess the legality, necessity, and proportionality of the request in accordance with applicable law. All approvals should be documented and maintained in the TPL. Exempted exchanges remain subject in full to the authentication, classification, encryption, audit, and TPL requirements of the Technical Specification, and should be recorded under the applicable non-consent authorisation basis in the Consent Policy Record.

9. Revocation

9.1 A citizen may revoke any consent at any time, without charge and without being required to state a reason, through any supported consent channel. Revocation takes effect immediately for future transactions: the consent artefact status should be set to REVOKED, the revocation should be propagated to the Consent Policy Registry, and subsequent requests referencing the revoked consent should be rejected within five (5) seconds (Technical Specification Section 10).

9.2 Revocation does not invalidate exchanges lawfully completed prior to its effect. Historical consent and transaction records remain auditable through the TPL notwithstanding revocation.

10. Consent Records and Retention

10.1 All consent transaction logs should be recorded and maintained by PDA, by the Platform Operator, and by the relevant Participating Entity for a period of not less than five (5) years from when the context expires, or such longer period as PDA may specify, for regulatory, audit, and non-repudiation purposes.

10.2 Access to consent records should be restricted to authorised personnel and should be made available to PDA, competent courts, and authorised investigative agencies upon request. Consent records should not contain the content of the data exchanged.

11. Delegated Channel Applications

11.1 Where a transaction is initiated through a Delegated Channel application, consent requirements are identical to those applicable to standard Participating Entity transactions. The consent notification should identify the sponsoring Participating Entity as the data accessor; the sponsoring entity is the accountable party, and the citizen's legal relationship is with the sponsoring entity, not the third-party application. The consent artefact and TPL record should nonetheless capture the full delegation chain for regulatory and audit purposes (Technical Specification Section 26.6).

11.2 In multi-party workflows, each required consent artefact should be collected independently, and no step requiring a party's consent should proceed until that party's artefact is active and valid.

12. AI Systems

12.1 Where an AI system acts as a Consumer on behalf of an institution, the consent model is unchanged: the citizen consents to the institution receiving the data for the declared purpose, and the institution remains accountable for ensuring its AI uses the data only as consented. AI-originated requests carry additional model-identifier and invoking-principal bindings recorded in the TPL (Reference Architecture Sections 12.2.1–12.2.2).

12.2 An AI agent shall not grant, initiate, or exercise consent on a citizen's behalf. Delegated consent for AI agents acting on behalf of citizens is not operationally enabled in WASL v1; any request presenting a delegated-consent artefact type should be rejected pending operationalization (Reference Architecture Section 12.3; Technical Specification Section 24.5).

13. Compliance, Governance, and Review

13.1 A departure from this Guideline should be documented and justified. Where the Regulations make consent mandatory for the data concerned, non-observance may also constitute non-compliance with the Regulations and attract the applicable audit, enforcement, suspension, and penalty provisions as specified in the Regulations.

13.2 PDA owns and governs this Guideline and the consent framework. NADRA, as Platform Operator, operates the consent management infrastructure under PDA's governance. Consent Policy Records published in the Consent Policy Registry are the machine-enforceable expression of this Guideline and should be maintained consistent with it.

13.3 This Guideline should be reviewed by PDA at least once every review cycle applicable to the Reference Architecture, and in any event upon material amendment of the Regulations, the Reference Architecture, or the Technical Specification. Amendments follow the issuance procedures of DNP-X.001 FWK.