

## Summary of DSCI's Submissions on the IRDAI's Consultation Paper titled 'Public Insurance Registry - Digital Public Infrastructure for Insurance'

The Data Security Council of India ("DSCI") provided stakeholder inputs on the Insurance Regulatory and Development Authority of India's ("IRDAI") consultation paper, titled "[Public Insurance Registry – Digital Public Infrastructure for Insurance](#)" ("Consultation Paper"). DSCI acknowledges the Consultation Paper's objective of establishing the Public Insurance Registry ("PIR") as a digital public infrastructure for insurance, supported by a standardized and interoperable data ecosystem. The proposed framework adopts a privacy-centric, consent-based, and federated architecture, while promoting financial inclusion, consumer trust, and streamlined access to insurance through phased implementation under IRDAI governance.

While supporting these objectives, DSCI has offered targeted recommendations, confined to matters within DSCI's areas of work, namely data protection, cyber security, artificial intelligence, emerging technologies and the digital economy, and directed principally at points where further articulation may assist participants in implementing the framework consistently with the wider body of law to which they are already subject.

### Cross-Insurer Rights Requests

**Gap and Issue:** Rights requests may only reach the relevant insurer, limiting cross-insurer corrections. Shared updates could also create account-takeover risks and delay identification of affected policyholders after service-provider incidents.

**DSCI Recommendation:** The framework could enable a single correction request to reach all relevant insurers, subject to risk-based authentication. PIR and service-provider records may also help identify affected insurers and policyholders faster.

### Broader Ecosystem Participation

**Gap and Issue:** Key ecosystem participants, such as Third Party Administrators, vendors, InsurTechs, Account Aggregators, and Consent Managers, are not comprehensively addressed despite their role in processing policyholder data.

**DSCI Recommendation:** Baseline security and data-protection expectations could be extended to ecosystem participants through third-party risk frameworks. The framework may also support interoperability, open standards, and controlled sandbox access.

### Privacy-Preserving Data Architecture

**Gap and Issue:** The proposed architecture lacks a common baseline for privacy and security controls and does not clearly define PIR data-retention and governance requirements.

**DSCI Recommendation:** A common baseline of privacy and security measures could be established, including tokenization, pseudonymization, and purpose-based access controls. PIR may retain only the minimum data required for discovery, access, and audit functions.

## Purpose-Bound Identity References

**Gap and Issue:** The framework does not clarify permissible uses of PIR identifiers or the treatment of low-confidence matches, creating risks of misuse and inaccurate record linkage.

**DSCI Recommendation:** PIR identifiers could be made strictly purpose-bound, with low-confidence matches requiring verification before any consequential action. Authentication requirements may be risk-based and outcome-focused.

## Standardized Insurance Data

**Gap and Issue:** Standardization focuses on formats and fields but lacks a clear data-and-purpose taxonomy and sufficient consideration of operational data flows and legacy records.

**DSCI Recommendation:** The framework could adopt a data-and-purpose dictionary and align standards with actual data flows. Legacy-data updates may be conducted through authenticated insurer-led outreach.

## Consent and Data Protection

**Gap and Issue:** The framework does not clearly map processing activities to grounds under the [Digital Personal Data Protection Act, 2023](#) ("DPDP") or sufficiently address consent, transparency, access visibility, and breach-notification responsibilities.

**DSCI Recommendation:** Processing activities could be mapped to applicable DPDP grounds, with provisions for granular consent, transparency, access-history visibility, and clearly allocated breach-notification obligations.

## Commercial Confidentiality Safeguards

**Gap and Issue:** The framework does not fully address evolving re-identification risks, dataset segregation, conflicts of interest, or technology-provider concentration risks.

**DSCI Recommendation:** Privacy safeguards could be periodically reviewed and independently tested. Additional measures may include access audit trails, conflict-management controls, and technology-neutral certification mechanisms.

## Significant Data Fiduciary Readiness

**Gap and Issue:** The framework references potential Significant Data Fiduciary status but does not clarify interim governance expectations or alignment with DPDP obligations.

**DSCI Recommendation:** PIR could voluntarily align with Significant Data Fiduciary requirements from inception, including independent audits, impact assessments, and appropriate governance mechanisms.

## Broader Regulatory Oversight

**Gap and Issue:** The framework provides limited clarity on oversight of interoperability, innovation, privacy, security, fraud prevention, and model governance.

**DSCI Recommendation:** Oversight dimensions could be clearly defined with transparent indicators. Model methodologies may be documented and periodically reviewed, supported by tamper-evident audit logs.

### **Adaptive Privacy and Security**

**Gap and Issue:** The framework does not explain how privacy and security safeguards will evolve to address emerging threats such as deepfakes, synthetic media, and synthetic identities.

**DSCI Recommendation:** The architecture could adopt modular and updateable security controls. PIR may periodically reassess threats, conduct independent testing, and publish outcome-based security and resilience metrics.