Policy Statement on "DoT's SIM Binding Directions"
Data Privacy Bharat Center (DPBC)
A Public Interest Policy Think Tank on Data Governance & Digital Rights

Data Privacy Bharat Center (DPBC) takes note of the recent directions issued by the Department of Telecommunications (DoT) under the Telecom Cyber Security (TCS) Rules, 2024, mandating continuous SIM binding and periodic web-session logout for app-based communication services using Indian mobile numbers.

From a public policy perspective, this measure represents a structural intervention aimed at strengthening telecom identifier integrity. The stated objective—to prevent misuse of Indian mobile numbers in phishing, impersonation, digital arrest scams, and cross-border financial fraud—addresses a demonstrable and escalating risk within India's digital ecosystem. DPBC recognises the legitimacy of this regulatory objective and the need to recalibrate authentication standards considering evolving cybercrime models.

The introduction of continuous SIM-device linkage and time-bound web re-authentication marks a shift from one-time verification models to ongoing identity anchoring. If implemented effectively, this framework has the potential to reduce persistence of compromised accounts, raise operational costs for fraud networks, and improve traceability of telecom identifiers without altering encrypted content architecture.

However, DPBC underscores that regulatory effectiveness must be balanced with constitutional safeguards and data protection principles. Implementation should remain narrowly tailored to identifier misuse and must not inadvertently expand metadata collection beyond necessity. Any authentication-layer enhancements should adhere to data minimisation, purpose limitation, and storage limitation standards, with clear user-facing disclosures and documented privacy impact assessments.

Importantly, encryption protections must remain intact. Telecom-layer accountability should not translate into content-layer intrusion.

DPBC recommends issuance of detailed technical implementation guidelines, clarity on retention parameters, and periodic public reporting on measurable fraud reduction outcomes. Evidence-based evaluation will be critical to ensuring proportionality and maintaining digital trust.

Cybersecurity resilience and privacy protection are mutually reinforcing pillars of responsible digital governance. With calibrated implementation and transparent oversight, this framework can contribute to both fraud mitigation and rights-preserving innovation within India's digital ecosystem.