

Summary - DSCI's Submission on Draft Amendments to Aadhaar Good Governance Rules, 2020

The Data Security Council of India (DSCI) submitted its comments on the draft amendments to the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020, welcoming the government's intention to expand the scope of Aadhaar authentication to Private Entities (PEs). DSCI appreciates this move as a progressive step that could enhance innovation, improve service delivery, and deepen digital inclusion across sectors.

While supporting the amendment in principle, DSCI highlighted the following privacy, security, and governance concerns that need to be addressed before implementation:

1. Need for a Strong Privacy and Cybersecurity Framework

The draft does not clearly define the privacy and security standards that private entities must adhere to while conducting Aadhaar authentication.

Recommendations:

- Establish a governance mechanism to oversee the purpose-specific use of Aadhaar authentication by private entities.
- Mandate privacy-preserving technologies and data minimization principles to prevent misuse or over-collection of personal data.
- Require regular vulnerability assessments and secure data transmission protocols to prevent breaches.
- Clarify that no Aadhaar data should be retained by private entities, except for limited purposes directly linked to authentication outcomes.

2. Clarifying Roles and Oversight Mechanism

It was observed that the draft amendments lacked clarity on the role of referring Ministries or Departments, especially in cases where a private entity falls under the jurisdiction of multiple regulators (e.g., a Fintech entity offering both insurance and payments). Therefore, it was suggested that the amendments may

- Clearly assign responsibility to specific Ministries or Departments for each category of private entity.
- Define regulatory accountability for compliance enforcement, post-authentication approval.

2. Defining Eligibility and Scope of Use

It was also observed that the terms such as “ease of living” and “better access to services” remain undefined, which may lead to ambiguities in identifying eligible private entities.

Recommendation:

- Elaborate on these terms in the Rules to help streamline proposals and approval processes.
- Introduce guidelines to assess proposals, ensuring Aadhaar authentication is used only where necessary and beneficial to residents.

Conclusion

DSCI supports the government's vision of expanding Aadhaar's utility as a trusted digital identity layer, especially for private sector-led innovation. However, the implementation must be backed by robust data protection norms, purpose limitation principles, and cyber resilience standards. A well-calibrated framework will ensure that Aadhaar remains a secure and equitable tool for digital governance and service delivery in India.