

EU-IN TTC Business Forum

Fostering EU-IN Tech Business Cooperation under the Trade and Technology Council

Plenary V: Cybersecurity and Data Governance: The Trust Layer for Cross-Border Business

Date: 4 June 2026 | Time: 03:00 AM – 03:45 AM

Location: Shangri-La Eros, New Delhi

Esteemed speakers

1. Mr. Nishad Ali, CEO of Teltonika
2. Mr. Atul Kumar, Director – Government Initiatives and Global Trade at Data Security Council of India (DSCI)
3. Dr. Sanjay Bahl, Director General at from Indian Computer Emergency Response Team (CERT-IN)
4. Mr. A.K. Tiwari, President (Regulatory and Policy), Reliance Jio

Moderator

Kristina Brazevic, Economic Counsellor at Embassy of Lithuania in New Delhi

Key Recommendations

1. Explore mutual recognition or fast-track pathways between Indian frameworks such as Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) and EU certification frameworks to reduce the existing 12-16 month timelines for accreditation.
2. Formalise bilateral CERT-In and EU CERT cooperation for real-time threat intelligence sharing and coordinated incident response.
3. Conduct coordinated cyber crisis simulation exercises across EU-India economies to assess resilience maturity and build institutional ties.
4. Develop tailored frameworks (under the TTC) helping SMEs navigate DPDPA-GDPR compliance without the legal and technical resources available to large enterprises.
5. Align on 3GPP and related standards through joint advocacy to ensure open and compatible standards that benefit both markets and can be replicated in third countries.
6. Establish joint sandbox environments for AI testing and bias auditing.

Discussion Summary

1. India's Data Governance Architecture

Mr. Atul Kumar (DSCI) outlined India's multi-layered approach to data governance describing four interconnected pillars:

- The Digital Personal Data Protection Act (DPDPA) as the overarching legislative framework
- Sector-specific regulations from bodies such as the Reserve Bank of India (RBI), SEBI, and IRDAI, each with distinct data handling requirements
- Proactive institutional actors — particularly CERT-In and NCIIPC — providing advisories, hands-on support, and driving cyber resilience at scale
- Digital Public Infrastructure (DPI) as a structural foundation, with privacy and data governance embedded by design into identity and data-sharing architectures

Mr. Kumar noted that this layered ecosystem has helped position India as a global hub for security operations, GCC (Global Capability Centres), and product security development. He emphasised the shift in the cybersecurity paradigm from compliance-based, point-in-time audits to real-time, continuous monitoring and resilience — a transition now embedded across India's national and sectoral governance frameworks.

2. Building Trusted and Resilient Digital Ecosystems

Dr. Sanjay Bahl (CERT-In) identified five foundational elements for cross-border digital trust:

- Shared cybersecurity standards and frameworks — noting strong uptake of ISO/IEC 27001 among companies operating across both markets as a baseline for mutual assurance
- Cert-to-Cert cooperation — trusted institutional channels for incident response, threat intelligence sharing, and joint crisis management
- Public Key Infrastructure (PKI) ecosystems — citing India's Controller of Certifying Authorities (CCA) and comparable EU frameworks as essential to legally valid cross-border transactions
- Risk-based approaches to AI governance — highlighting India's participation in ANSI-led frameworks and the importance of joint AI bias and testing methodologies
- Capacity building — acknowledging the EU's strength in regulatory enforcement and the value of knowledge transfer, particularly as emerging technologies including AI, quantum computing, 6G, and IoT continue to converge

3. Trusted Infrastructure for Secure Connectivity

Mr. Tiwari (Reliance Jio) spoke from the vantage point of India's largest digital connectivity provider, managing 524 million customers across 1.5 million 5G and 4.6 million 4G sites. He identified five critical building blocks for trusted digital infrastructure:

- ☐ Security by design — embedding security at every component, layer, and equipment level from the outset, rather than as a retrofit
- ☐ Resilience — continuous investment in network upgrades, recognising that threat actors consistently evolve ahead of defensive measures
- ☐ Open architecture — enabling subsea cable and terrestrial network diversification, reducing single points of failure, and supporting supply chain resilience
- ☐ Indigenous, trusted-source equipment — aligned with Government of India mandates on trusted telecom infrastructure
- ☐ DPDPA and GDPR convergence — noting significant alignment in user-rights orientation between both frameworks, and flagging SME cross-border business models as a key opportunity area for TTC focus

4. Business Experience: Compliance as Competitive Advantage

Mr. Nishad Ali(Teltonika) offered a practitioner's perspective on scaling an IoT company from Lithuania across the Indian market. He described the company's journey from entering India in 2020 — with one salesman and one engineer — to a team of 27 professionals today, with three products approved under India's National Security Directive and 39 certified under MTCTE.

His central argument reframed the compliance discussion:

- ☐ Early market entrants without certification standards gradually exited — not due to market contraction (the IoT sector was growing) but because they could not sustain certification requirements
- ☐ Compliance is not a cost of doing business. It is a company's signature — the instrument of trust that unlocks access to healthcare, transportation, critical infrastructure, and smart city markets
- ☐ In high-stakes use cases — remote robotic surgery over private 5G, AI-managed traffic signals across 200 junctions — a data breach or network intrusion is not a business problem. It is a safety and potentially life-threatening failure

He identified certification timelines as the primary friction point for EU-India cross-border business. His MTCTE certification required 16 months — a delay that effectively postponed the wider ecosystem deployment by two years. He called for a shared vocabulary, faster cross-border certification pathways, and potentially a sandbox framework for industrial IoT testing.