To: Ambassador of the European Union to India

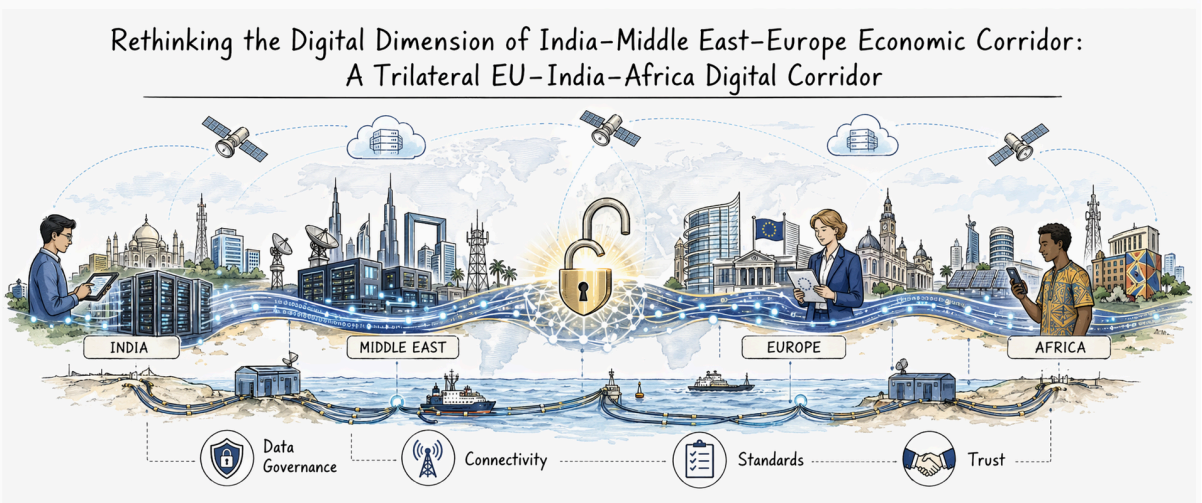
From:

***Ananya Srivastava**, MSc Sustainable Management & Eco-Innovation*
Rennes School of Business, France

***Sanyam Bajaj**, Co-Founder, The EU-India Watch*
&
Verena Zimmer, Country Manager Asia at the Stuttgart Region Chamber of Commerce

(EU-India Young Leaders Cohort 2026)

Date: 23.04.26



Subject: *Repositioning the India–Middle East–Europe Economic Corridor (IMEC) as a trilateral digital governance framework co-designed with African partners, with credibility as the precondition for scale*

Executive Summary

The India–Middle East–Europe Economic Corridor (IMEC) is an inter-regional economic integration project proposed in 2023 by the United States in cooperation with India, the European Union, and several Middle Eastern partners (Liang 2025). It is currently framed as the alternative infrastructure network, with digital infrastructure treated as a subsidiary trade-facilitation layer (Liang 2025). In this context, while the European Union has been linking the EU Digital Single Market with Digital India, it should consider the corridor's digital dimension not as a technical interoperability question, but as a strategic instrument for repositioning EU–India cooperation as a rights-based, trilateral offer to African partners (European Commission 2025c). This positioning can also support broader Global Gateway objectives and reinforce the EU's role as a trusted digital partner in the Global South.

At the same time, the value of this offer for African jurisdictions and for the EU–India relationship itself depends on a principle that should guide implementation from the outset: credibility before scale (Atlantic Council 2025; European External Action Service and European Commission 2025).

Introduction

On 9 September 2023, IMEC was announced at the G20 New Delhi Summit as a multimodal corridor linking India to Europe through the Gulf, with transport, energy, and digital connectivity as its three declared pillars (India–Middle East–Europe Economic Corridor n.d.). The announcement carried evident geopolitical intent: to signal that an alternative to Chinese-led connectivity was not only conceivable but institutionally realisable. Two years on, that signal has not been backed by substance. Official and analytical attention has remained concentrated on logistics and energy, and the digital pillar, although regularly invoked, has yet to be translated into a governance proposition commensurate with the corridor's stated ambitions (Atlantic Council 2025; ORF Middle East 2025).

The cost of that gap has grown as the strategic environment has shifted. The United States, once the initiative's principal political sponsor, has become a less predictable partner for both the EU and India under conditions of renewed transatlantic friction (Bomassi 2026). China, meanwhile, continues to deepen its export of state-backed digital infrastructure across Africa and parts of Asia through the Belt and Road Initiative, consolidating both technical dependencies and governance norms that are difficult to reverse once embedded (The Roosevelt Group 2025). In this context, the EU and India are increasingly identified in international discourse as the most credible potential co-architects of a third model, one grounded in open-source, interoperable, and rights-respecting digital infrastructure (European Commission 2025b; Teevan and Pouyé 2025). President von der Leyen's formulation at the January 2026 EU–India leaders' meeting, linking Indian "skills, services and scale" with European "technology, capital and innovation," reflected a political consensus that now needs institutional translation (European Commission 2026a).

That translation has, in part, already begun. The *Towards 2030* Joint EU–India Comprehensive Strategic Agenda commits both partners to strengthening mutual experience sharing on universal and secure digital infrastructure and to developing trusted telecommunications ecosystems as a shared strategic priority (European Commission

2026b, §2.2.4). It tasks both sides with deepening collaboration under IMEC specifically to diversify trade routes, reduce strategic dependencies, and future-proof supply chains across maritime, rail, digital, and energy dimensions (European Commission 2026b, §4.1.2). And it advances the EU–Africa–India Digital Corridor within the IMEC framework — anchored in part by the Blue Raman submarine cable system — as the operational vehicle for secure, resilient, and high-capacity data connectivity across the corridor (European Commission 2026b, §4.1.3). These are not aspirational formulations. They are formally agreed commitments, and they define the floor of ambition against which this memo's recommendations are calibrated.

The argument advanced here is that IMEC provides the most concrete existing institutional scaffolding through which this third model could be operationalised, but only if four credibility conditions are addressed openly rather than glossed over. The memo proceeds by setting out the policy problem, analysing those conditions in turn, and offering five recommendations calibrated to distinct institutional actors.

Policy Problem and Analysis

The immediate policy problem is that IMEC's current digital conversation is framed almost entirely around efficiency. The Atlantic Council has argued that realising IMEC's potential requires corridor-wide interoperability, common digital platforms, and harmonised governance standards (Atlantic Council 2025). ORF Middle East estimates that trade and customs digitisation alone could cut import compliance times by roughly half and deliver cost savings of twenty to fifty percent (ORF Middle East 2025). These are meaningful gains. They are not, however, a governance proposition, and they do not address the question of what model of digital infrastructure IMEC is implicitly exporting to third jurisdictions through its operational choices. A credible governance proposition would need to go further: leveraging digital governance as a transparency mechanism to reduce compliance risks and informational asymmetries that currently hinder European private sector investment, while ensuring that data privacy protections for all partner jurisdictions are embedded from the outset rather than treated as an afterthought.

From an EU–India perspective, the strategic significance of the corridor lies in complementarity: India brings implementation scale and an established presence across African digital infrastructure, while the EU brings the world's most comprehensive rights-based regulatory framework. Neither bloc individually can offer African partners a credible alternative to existing digital infrastructure paradigms, but together, and within an institutional frame such as IMEC, they plausibly can. India has, in under a decade, built and scaled the world's largest digital public infrastructure stack, lifting formal banking inclusion from twenty-five percent in 2008 to over eighty percent by 2023 (Carnegie Endowment for International Peace 2025). That model already has traction in Africa: nine of the eleven countries implementing the Modular Open-Source Identity Platform are on the continent, and India extended over USD 13 billion in concessional aid to African projects between 2010 and 2024 (IMPRI 2025). The EU, in parallel, has developed the most robust rights-based digital regulatory architecture globally through the GDPR, the Digital Services Act, and the AI Act. What IMEC offers is the institutional frame through which India's proven implementation

capacity and the EU's regulatory credibility can be brought together into a single, coherent offer.

The credibility of that offer, however, is contingent on four conditions that remain unaddressed.

Condition 1: India's digital public infrastructure carries unresolved exclusion by design

India's digital public infrastructure is not the unqualified success frequently presented in international fora. Unique Identification Authority of India's (UIDAI) own parliamentary submissions indicate that approximately 312 million Aadhaar biometric authentications are attempted monthly, of which roughly 20.3 million fail, a 6.5 percent failure rate that has remained unchanged for over a decade (Policy Circle 2026). Independent research has documented biometric match failure rates as high as forty-nine percent in Jharkhand and thirty-seven percent in Rajasthan, according to government-reported data (Dixon 2017), figures corroborated by India's own Parliament, whose Public Accounts Committee heard in 2025 that biometric failures continue to exclude eligible welfare beneficiaries at scale (Biometric Update 2025). These are not transitional implementation costs. They are a design outcome, and they fall disproportionately on manual labourers, the elderly, and those whose biometrics degrade with physical work (Carswell, De Neve, and Ponnarasu 2021; Muralidharan, Niehaus, and Sukhtankar 2020). A further complication arises from India's recent decision to open Aadhaar infrastructure to select private facial authentication firms under a regulatory sandbox, which introduces the prospect of private surveillance legitimised through public infrastructure (Huynh 2025).

Condition 2: The EU's regulatory credibility is under internal pressure.

The EU's regulatory credibility, which is the very comparative advantage it brings to this proposition, is currently under internal pressure. On 19 November 2025, the European Commission published its Digital Omnibus package, amending the GDPR, the AI Act, and adjacent legislation (European Commission 2025a). The Jacques Delors Centre has concluded that the package, although framed as a technical simplification exercise, contains substantive changes that could weaken fundamental rights safeguards and, in markets dominated by foreign technology companies, risk entrenching rather than challenging the concentration of platform power (Jacques Delors Centre 2026). The proposal also weakens AI Act transparency provisions, including the requirement that providers publish their own high-risk system assessments on an EU database (Amnesty International 2026). The credibility of any rights-based offer made to African partners will be shaped materially by how these proposals are resolved through trilogue.

Condition 3: African jurisdictions must be co-designers, not recipients.

African jurisdictions therefore must be positioned as co-designers rather than recipients. The African Union's Digital Transformation Strategy for Africa (2020–2030), anchored in a Digital Single Market vision, harmonised policies, and interoperable digital public goods, pre-dates the IMEC digital conversation and must serve as the foundational framework for any trilateral architecture (African Union 2020; Bahru 2026). A corridor that treats African states as

demonstration sites for EU–Indian infrastructure will fail both politically and substantively. It would also replicate, in different geometry, the extractive North–South knowledge flows that a rights-based alternative is meant to displace.

Condition 4: The hardware gap remains unaddressed.

A fourth structural condition cuts across all three. Digital governance frameworks, however rights-respecting, are software solutions. Africa's primary digital deficit remains hardware: fiber-optic cables, data centers, and reliable power infrastructure. China, through the Digital Silk Road, has spent over a decade filling precisely that gap, laying physical infrastructure across the continent at speed and cost that Western alternatives have not matched (The Roosevelt Group 2025). An EU–India offer grounded exclusively in regulatory standards and governance architecture, without a credible hardware commitment, risks being dismissed by African partners as procedurally sophisticated but practically inert. The Global Gateway financing recommendation below is designed to address this directly, but the hardware gap must be named as a credibility condition in its own right, not treated as an implementation detail.

Taken together, these four conditions constitute the logic behind the framing advanced in the executive summary: credibility before scale. The governing assumption should be that any expansion of the corridor's digital footprint must be matched, and in practice preceded, by visible progress on inclusion-by-design in India, regulatory baseline protection in the EU, and co-governance with African partners.

Policy Recommendations

To operationalise this framing while preserving the integrity of the broader IMEC agenda, the Delegation of the European Union to India should treat IMEC's digital dimension as the principal vehicle through which the EU–India relationship can offer a credible, trilateral alternative to existing digital infrastructure paradigms. The recommendations below are ordered by feasibility and calibrated to distinct institutional actors.

The Delegation should advocate the establishment of an IMEC Digital Governance Working Group by Q4 2026, with formal African Union representation rather than observer status. The Atlantic Council has already argued that IMEC requires a central coordinating body with ministerial, secretariat, and technical working-group components (Atlantic Council 2025). This memo extends that call by arguing that the governance architecture must embed African co-design from the outset. The working group should have a clear mandate covering interoperability standards, algorithmic accountability, and exclusion-audit protocols, and it should report annually to the EU–India Trade and Technology Council and to the African Union Commission in parallel.

EU Global Gateway digital financing efforts directed toward IMEC-adjacent initiatives should be conditioned on alignment with the African Union–endorsed standards for digital identity, payments, and data governance (Bahru 2026). The gap between stated ambition and actual commitment is substantial: at the most recent EU-Africa Business Forum, less than EUR 1 million of the roughly EUR 590 million pledged in public-private financing was extended for digitalisation (CSIS 2025). Conditioning disbursements on AU standards compliance would

operationalise co-design rather than invoke it rhetorically, and it would provide the EU with a practical instrument for differentiating Global Gateway from both US platform exports and Chinese infrastructure financing, offering African partners a rights-based, concessional alternative to debt-heavy models that embed long-term technical and governance dependencies (The Roosevelt Group 2025; CSIS 2025)

The Delegation should advocate the adoption of binding exclusion-audit requirements for any digital public infrastructure deployed under a trilateral framework. Whether the system is MOSIP-based[1], UPI-based[2], or otherwise, published failure rates disaggregated by age, occupation, and disability status should be a condition of deployment. The existing research base on Indian DPI exclusion provides a methodological foundation (Muralidharan, Niehaus, and Sukhtankar 2020; Carswell, De Neve, and Ponnarasu 2021). This recommendation is particularly significant because it addresses the credibility gap most visible to African civil society and most easily exploited by competing infrastructure models.

The Delegation should coordinate closely with EU institutional actors to protect the regulatory baseline during the Digital Omnibus trilogue. Amendments that weaken AI Act transparency provisions or narrow the definition of personal data under GDPR Article 4 should be resisted on the grounds that they compromise not only internal EU rights protection but also the external credibility of the EU–India offers to African partners (Jacques Delors Centre 2026; Amnesty International 2026). This is, admittedly, a recommendation that extends beyond the Delegation's immediate mandate, but the external consequences of the Omnibus trajectory are real and should inform the Delegation's internal advocacy within the Commission.

The Delegation should propose the commissioning of an independent annual review, published jointly by an EU institution, an Indian institution, and an African Union body, tracking implementation, exclusion metrics, and governance outcomes across the corridor. Accountability mechanisms that sit with only one party will not be credible to the other two. This review should become the primary public-facing document through which the corridor's credibility is tested and, over time, earned.

At the same time, none of these recommendations alone will be sufficient. The trilateral corridor framing is a strategic orientation rather than a single policy instrument, and it will succeed only if the EU and India are willing to apply to themselves the same standards they encourage African partners to embrace. This is the substantive content of credibility before scale, and it is the condition on which the broader proposition rests. This trilateral approach offers a competitive alternative to debt-heavy infrastructure models by focusing on concessional financing and the harmonization of regulatory baselines

[1] MOSIP-based refers to digital identity systems built on the Modular Open-Source Identification Platform (MOSIP)

[2] UPI-based refers to the Unified Payments Interface, a real-time digital payment system developed by NPCI that allows instant interbank transactions via mobile devices

Conclusion

IMEC offers the European Union an opportunity to align an existing connectivity initiative with a more ambitious digital governance agenda, one the *Towards 2030* Strategic Agenda has already formally committed the EU and India to pursuing with Africa at its core. For the Delegation of the European Union to India, the central policy task is to frame the corridor's digital dimension not as a technical trade-facilitation workstream, but as the institutional vehicle through which a democratic trilateral alternative can be built with African co-design at its core. The window is narrow. If the EU and India act within it, the corridor offers a credibility neither the US nor China can provide. If they do not, IMEC's digital dimension will be absorbed into existing paradigms and the opportunity will close. The governing principle should be straightforward: credibility first, scale second.

References

African Union. 2020. *The Digital Transformation Strategy for Africa (2020–2030).* Addis Ababa: African Union Commission. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

Amnesty International. 2026. "How EU Proposals to 'Simplify' Tech Laws Will Roll Back Our Rights Online to Feed AI." April. https://www.amnesty.org/en/latest/news/2026/04/eu-simplification-laws/

Atlantic Council. 2025. "The India–Middle East–Europe Economic Corridor: Connectivity in an Era of Geopolitical Uncertainty." November 7. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-india-middle-east-europe-economic-corridor-connectivity-in-an-era-of-geopolitical-uncertainty/

Bahru, Yinebeb. 2026. "Africa Should Invest in Digital Public Infrastructure to Aid Regional Integration." Africa at LSE. March 17. https://blogs.lse.ac.uk/africaatlse/2026/03/17/africa-should-invest-in-digital-public-infrastructure-to-aid-regional-integration/

Biometric Update. 2025. "High Rates of Aadhaar Biometric Verification Failure Leads to UIDAI Scrutiny." July 18. https://www.biometricupdate.com/202507/high-rates-of-aadhaar-biometric-verification-failure-leads-to-uidai-scrutiny

Bomassi, Lizza. 2026. "Living with Friction: Three Anchors of the EU-India Partnership." EUISS Brief No. 2. European Union Institute for Security Studies, January. https://www.iss.europa.eu/publications/briefs/living-friction-three-anchors-eu-india-partnership

Carnegie Endowment for International Peace. 2025. "Digital Public Infrastructure: A Practical Approach for Africa." February. https://carnegieendowment.org/research/2025/02/digital-public-infrastructure-a-practical-approach-for-africa

Carswell, Grace, Geert De Neve, and Subramanian Ponnarasu. 2021. "Transparency, Exclusion and Mediation: How Digital and Biometric Technologies Are Transforming Social Protection in Tamil Nadu, India." Oxford Development Studies. https://www.tandfonline.com/doi/full/10.1080/13600818.2021.1904866

CSIS (Center for Strategic and International Studies). 2025. "Global Gateway's Infrastructure Plan for Africa Announced at EU–AU Summit." November 6. https://www.csis.org/analysis/global-gateways-infrastructure-plan-africa-announced-eu-au-summit

Dixon, Pam. 2017. "A Failure to 'Do No Harm' — India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S." Health and Technology 7 (4). https://pmc.ncbi.nlm.nih.gov/articles/PMC5741784/

European Commission. 2025a. "Digital Package: Digital Omnibus and Digital Omnibus on AI Regulation." November 19. https://digital-strategy.ec.europa.eu/en/faqs/digital-package

European Commission. 2025b. "Key Outcomes of the Second EU–India Trade and Technology Council." February 28. https://digital-strategy.ec.europa.eu/en/news/key-outcomes-second-eu-india-trade-and-technology-council

European Commission. 2025c. "EU-India Discuss Progress in Shared Digital Priorities." October 31. https://digital-strategy.ec.europa.eu/en/news/eu-india-discuss-progress-shared-digital-priorities

European Commission. 2026a. "Statement by President von der Leyen with President Costa at the EU–India Leaders' Meeting." January 26. https://ec.europa.eu/commission/presscorner/detail/en/statement_26_210

European Commission. 2026b. "Towards 2030: A Joint European Union-India Comprehensive Strategic Agenda." January 27. https://ec.europa.eu/commission/presscorner/detail/en/statement_26_224

European External Action Service, and European Commission. 2025. "The European Union and India — Strategic Agenda." September 17. https://www.eeas.europa.eu/sites/default/files/2025/documents/JOIN_2025_50_1_EN_ACT_part1_v9.pdf

Huynh, Haakon. 2025. "Public Infrastructure and Private Surveillance in India's Aadhaar System." TechPolicy.Press. August 18. https://www.techpolicy.press/public-infrastructure-and-private-surveillance-in-indias-aadhaar-system/

IMPRI Impact and Policy Research Institute. 2025. "India–Africa: Leveraging Digital Public Infrastructure for Economic Growth." October 3. https://www.impriindia.com/insights/india-africa-digital-economic-growth/

India–Middle East–Europe Economic Corridor. n.d. "About IMEC." https://www.imec.international/

Jacques Delors Centre. 2026. "The EU's Digital and AI Omnibus Is Heading in the Wrong Direction." https://www.delorscentre.eu/en/publications/detail/publication/the-eus-digital-and-ai-omnibus

Liang, Qin. 2025. "From Conception to Stalemate: An Assessment of the India–Middle East–Europe Economic Corridor (IMEC)." *Bulletin of the Institute of Oriental Studies* 5. https://banberorient.sci.am/index.php/bios/article/view/134

Muralidharan, Karthik, Paul Niehaus, and Sandip Sukhtankar. 2020. "Identity Verification Standards in Welfare Programs: Experimental Evidence from India." NBER Working Paper No. 26744. National Bureau of Economic Research.

ORF Middle East. 2025. "Digital Interoperability and Trade Facilitation in the India–Middle East–Europe Corridor." November 14. https://orfme.org/expert-speak/digital-interoperability-and-trade-facilitation-in-the-india-middle-east-europe-corridor/

Policy Circle. 2026. "Aadhaar Authentication Failures Trigger an Invisible Exclusion Crisis." April. https://www.policycircle.org/opinion/aadhaar-authentication-failures/

The Roosevelt Group. 2025. "The Digital Silk Road: China's Technological Engagement in Africa." March 10. https://roosevelt-group.org/quick-takes/the-digital-silk-road-chinas-technological-engagement-in-africa

Teevan, Chloe, and Romaric Pouyé. 2025. *From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure.* ECDPM Discussion Paper No. 384. European Centre for Development Policy Management. https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf