Strengthening Data Governance and Digital Trade in the Mekong Region: From Policy Frameworks to Operational Practice

From Policy Frameworks to Operational Practice - a capacity-building initiative delivered by Dr Anna Mysyshyn, Director of the Institute of Innovative Governance, in partnership with the Asian Development Bank, for government representatives across Cambodia, Thailand, China, and Laos.

Bridging Policy and Practice in the AI Era

The trainings focused on a central challenge facing governments globally: how to design digital trade systems that are not only efficient and interoperable, but also secure, resilient, and trusted in an era of rapidly evolving AI-enabled risks. This is no longer a theoretical concern — it is an operational imperative that demands immediate, structured responses from policymakers and technical stakeholders alike.

The programme combined legal, technical, and policy perspectives, translating international frameworks into practical tools applicable within institutional and regulatory contexts. Rather than presenting regulatory standards in isolation, each session was designed to connect the "what" of compliance with the "how" of real-world implementation — creating actionable pathways for government institutions at varying stages of digital maturity.

GDPR

General Data Protection Regulation — the global benchmark for data protection rights, lawful processing, and accountability obligations.

EU AI Act

The world's first comprehensive AI regulation, establishing risk-based obligations for developers, deployers, and users of AI systems.

DORA

Digital Operational Resilience Act — mandating ICT risk management and incident reporting for financial entities operating in digital environments.

UK Digital Trade Framework

The United Kingdom's approach to digital trade and cyber resilience, offering a complementary model to EU regulation with a focus on interoperability.

Ukraine's Operational Experience

Front-line lessons from responding to AI-enabled cyber and information threats, providing a critical real-world reference for risk-based governance design.

By grounding discussions in both regulatory frameworks and real-world implementation scenarios, the sessions aimed to move beyond conceptual compliance toward genuine operational readiness — equipping participants with the tools to respond dynamically to emerging digital threats and opportunities.

From "Paper Compliance" to Operational Systems

One of the most significant themes woven throughout the training programme was the critical transition from formal regulatory alignment to practical, institution-level implementation. Across the Mekong region — as in many parts of the world — governments have made considerable progress in adopting data protection laws and digital governance policies on paper. The harder and more consequential challenge is building the operational infrastructure to make those commitments real.

This practical orientation reflects a broader and accelerating shift in digital governance globally: from static compliance models to dynamic, risk-based systems capable of responding to AI-driven threats, including automated disinformation, data manipulation, and cyber-enabled economic risks. Participants explored concrete mechanisms for closing the gap between regulatory intent and institutional capacity.

Cross-Border Data Transfers

Secure and lawful mechanisms for enabling trusted data flows across jurisdictions, including adequacy decisions, standard contractual clauses, and binding corporate rules.

Data Protection Impact Assessments

Application of DPIAs in real institutional scenarios — moving beyond checkbox exercises to genuine risk identification and mitigation planning.

Interagency Coordination

Defining institutional roles, responsibilities, and escalation pathways to ensure coordinated responses to data incidents and cross-border regulatory questions.


Incident Reporting Protocols

Development of incident reporting, escalation procedures, and cross-border cooperation mechanisms capable of functioning under real-time operational pressure.

Digital Trade as a Cross-Disciplinary Domain

The trainings made clear — and this is perhaps their most important structural insight — that digital trade governance can no longer be approached through a single disciplinary lens. The era of siloed regulatory thinking, where lawyers draft data laws without engaging with technical realities, or where engineers build systems without reference to legal obligations, must give way to deeply integrated, cross-functional governance models.
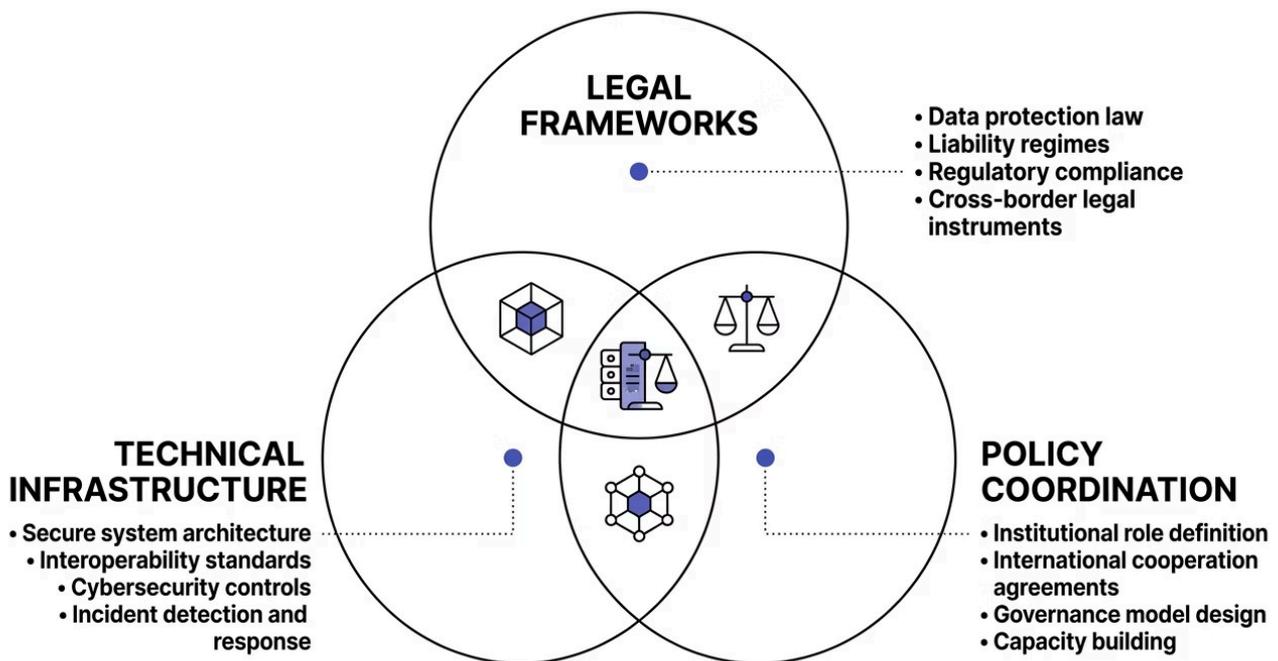
This convergence is particularly critical in the context of AI, where risks and opportunities span simultaneously across regulatory, technological, and geopolitical domains. An AI system deployed in cross-border digital trade may simultaneously raise questions of data sovereignty, algorithmic accountability, trade law obligations, and national security — demands that can only be addressed through coordinated, multi-disciplinary governance architectures.

For Mekong region governments, this means investing not only in individual expertise — skilled lawyers, competent technical officers, experienced policymakers — but in the institutional structures and inter-ministerial processes that allow these disciplines to work together effectively. The training programme modelled this integration throughout, deliberately mixing legal analysis, technical scenario work, and policy design exercises within each session.

Regional Momentum and the ASEAN Digital Economy Framework

The sessions engaged substantively with one of the most consequential ongoing regional developments: the ASEAN Digital Economy Framework Agreement (DEFA). DEFA represents a landmark commitment by ASEAN member states to create a harmonised, interoperable digital economic space — one capable of reducing regulatory fragmentation, lowering transaction costs, and enabling the kind of trusted data flows that underpin modern digital commerce.

Government representatives demonstrated a notably high level of preparedness and active engagement in shaping DEFA's implementation pathways. Discussions reflected not only policy ambition but also a clear and sophisticated focus on operationalisation — including infrastructure investment requirements, regulatory alignment strategies, and the institutional capacity needed to make commitments stick in practice.

Trusted Data Flows

Establishing transparent, secure, and legally sound mechanisms for cross-border data movement that businesses and citizens can rely upon.

Reduced Transaction Costs

Harmonised digital regulations and interoperable standards that lower the compliance burden for businesses operating across multiple ASEAN jurisdictions.

Predictable Regulatory Environments

Clear, consistent, and enforceable regulatory frameworks that give businesses the certainty they need to invest in and build digital trade operations.

This signals a significant and encouraging shift: digital trade governance in the region is evolving decisively from high-level political commitments toward practical systems with real operational content. The Mekong region is not merely observing global digital trade developments — it is actively shaping its own implementation pathways, informed by international best practice but grounded in regional realities and priorities.

AI, Accessibility, and Inclusive Digital Systems

In parallel with the core data governance training programme, Dr Mysyshyn contributed to a dedicated training on AI in trade organised by the Economic Research Institute for ASEAN and East Asia (ERIA). This session addressed a dimension of digital transformation that is too often treated as secondary to technical performance or regulatory compliance: the question of who benefits from AI-enabled digital trade systems, and whether those systems are genuinely accessible to all.

A key takeaway from this discussion was the importance of ensuring that AI systems are not only technically effective, but also secure, inclusive, and accessible. This extends well beyond the familiar categories of cybersecurity and performance optimisation. It encompasses digital inclusion — ensuring that small and medium enterprises, rural businesses, and less digitally mature institutions are not systematically excluded from the benefits of AI-enabled trade infrastructure.

Usability and equitable access are increasingly recognised as central, not peripheral, to sustainable digital transformation. An AI-powered customs clearance system that is technically sophisticated but practically inaccessible to small traders in remote areas does not advance digital trade — it deepens existing inequalities. These considerations are now being integrated into governance frameworks at both the national and regional level, and the ERIA training provided an important platform for surfacing them within an ASEAN context.

Principles for Inclusive AI in Trade

→ **Security by Design** — Building trustworthy AI systems from the ground up, not retrofitting security as an afterthought.

→ **Digital Inclusion** — Ensuring SMEs, rural operators, and less digitally mature institutions can participate meaningfully.

→ **Usability** — Designing interfaces and systems that work for real users across varying levels of technical literacy.

→ **Equitable Access** — Preventing AI-driven systems from concentrating benefits in large, well-resourced organisations.

Conclusion: Building Resilient Digital Economies

The Mekong region is demonstrating strong and increasingly well-grounded momentum in advancing digital trade and data governance frameworks. The training programme documented here delivered by the Institute of Innovative Governance in partnership with the Asian Development Bank reflects a model of capacity building that is both intellectually rigorous and practically oriented, moving participants from awareness to application across the full spectrum of digital governance challenges.

The trainings underscored a fundamental truth about building resilient digital economies in the current environment: regulatory alignment, while necessary, is not sufficient. Governments must move from the policy page to the operational floor — building institutions, teams, protocols, and technical systems that can respond dynamically to a threat landscape shaped by AI, geopolitical competition, and rapid technological change.

Operational Tools & Institutional Capacity

Investing in the practical infrastructure — human, technical, and procedural — that translates policy into reality.

Cross-Sector Collaboration

Breaking down disciplinary silos between legal, technical, and policy communities to build genuinely integrated governance systems.

Integration of AI, Cybersecurity & Data Governance

Treating these three domains not as separate policy areas but as a single, interconnected challenge requiring unified strategic responses.

Continuous Knowledge Exchange

Sustaining dialogue between regions — including Europe, Ukraine, and ASEAN — to ensure that operational lessons are shared and applied across institutional boundaries.

As digital trade systems become more complex and interconnected, capacity-building initiatives of this kind play a critical and irreplaceable role — supporting governments to move from policy design to effective, real-world implementation that delivers tangible economic and social benefits for all.