FUTURE OF PRIVACY FORUM

17TH ANNUAL ADVISORY BOARD MEETING

June 10–12, 2026 • Washington, D.C.

DATA TRANSFERS, LOCALIZATION & SOVEREIGNTY

Discussion Leads: Gabriela Zanfir-Fortuna + Matthew Reisman

SESSION DESCRIPTION

Caught between unpredictable geopolitics and the AI race, international data transfers are again at the epicenter of digital policymaking. Notions of data localization have been evolving into the more sophisticated "digital sovereignty", with governments in Africa, Asia, and the EU creating a kaleidoscope of policy and legal measures under this broad umbrella. At the same time, China is initiating a regional system for free data flows, and the US is insistently pushing the updated Global CBPR framework while limiting some transfers of sensitive data to adversary countries for national security purposes. Where does all this leave your compliance program and, more importantly, your data?

KEY DISCUSSION QUESTIONS

1. **How should senior privacy executives prepare for the future of transatlantic data flows in light of current uncertainties?** While the Transatlantic Data Privacy Framework was designed to be more durable than its predecessors, continuing tensions over U.S. surveillance law, the prospect of additional legal challenges to the framework in European courts, and broader transatlantic differences on digital policy have all placed stress on the DPF and raised questions about its future. How are senior privacy executives navigating this moment, and what contingencies should they have in place?
2. **Is the Global CBPR framework gaining enough traction to serve as a viable path for globally interoperable data flows, or are we heading toward a world of regional "clusters" - or an inevitable "spaghetti bowl" of bilateral arrangements?** The APAC region illustrates the divergence especially strongly: Singapore and Japan are active Global CBPR participants, whereas India, Vietnam, and Indonesia have recently strengthened localization requirements. More broadly, is the interoperability-through-mutual-recognition model (CBPR–and regional counterparts, e.g., ASEAN MCCs, Iberoamerican Model Transfer Agreement, AU Data Policy Framework) scaling fast enough to matter, or should privacy leaders building compliance programs plan for permanent fragmentation?
3. **The U.S. is simultaneously the world's strongest advocate for free data flows while operating a national security regime that restricts them. How do you reconcile these roles in your compliance program?** The DOJ's Data Security Program prohibits bulk transfers of sensitive personal data to six "countries of concern," including China and Russia, while the U.S. simultaneously champions the Global CBPR framework for trusted flows. For multinationals, these two vectors pull in opposite directions. How are organizations structuring governance to manage the national security compliance layer alongside traditional privacy transfer mechanisms?
4. **China's approach to cross-border data flows is in flux. How much do these signals of changes in direction matter for privacy professionals as they architect their compliance programs?** China was long viewed as one of the world's leading proponents of strict data localization practices, but has seemed intent on changing that perception, with the announcement of a "Global Cross-Border Data Flow Cooperation Initiative" in November 2024 and the launch of a "World Data Organization" in March 2026. What practical implications, if any, do these changes have for organizations?

PRE-READ DOCUMENTS (optional)

- Geopolitical Fragmentation, the AI Race, and Global Data Flows: The New Reality — Gabriela Zanfir-Fortuna & Christopher Kuner, FPF (2025).
- 2026: A Year at the Crossroads for Global Data Protection and Privacy – Gabriela Zanfir-Fortuna, FPF (2026)
- Cross-Border Data Flows in Africa: Examining Policy Approaches and Pathways to Regulatory Interoperability — Mercy King'ori, FPF (2025).