Briefing Note | **DataTalk** 17

Cross-border Privacy Rule Systems and Impacts on Financial Data in Asia

September 2022

Privacy protection rules around financial data in the Asia Pacific region has been a topic of interest for market participants and policymakers during a period of rapid change. The September session of DataTalk explored the intersection of cross-border privacy rules systems, data transfers, and financial data in APEC. The call covered key topics such as how firms view the likely route forward in the region, including lessons drawn from other jurisdictions. This note provides a summary of the discussion, respecting that the conversation was conducted under Chatham House Rule and comments are unattributed.

Knowing the existing frameworks is a necessary first step to building an adaptable and scalable framework that can be applied across multiple jurisdictions. Comparing the Asia Pacific Economic Cooperation (APEC) framework for cross-border privacy rules system to the EU and UK models is essential to understanding whether the principles are applicable across multiple jurisdictions, with differing rules systems and meeting regulatory obligations in each jurisdiction.

Understanding jurisdictional nuances is key for a dynamic model. Regulatory fragmentation is a challenge for firms operating across multiple jurisdictions, especially in APEC, where low standardization and fragmented requirements are likely to exist, creating challenges for the continued open and responsible flow of data. Frameworks applied in major markets, such as the EU GDPR, are being used as models for developing new laws. However, this practice pays insufficient attention to local factors which influence how data is collected, stored, shared, and used. This leads the industry to a conclusion: while similar concepts may apply globally, local market applicability requires nuance. A successful understanding of the differing legal and regulatory requirements makes for a framework that can be operationalized, and thus, one that can more nimbly react and respond to changing systems.

The amount of regulation covering personal data, especially financial data, continues to trend upward. Consequently, firms require a growing pool of talent to manage compliance and operational requirements. In the AI space, a redux of GDPR is likely given the numerous similarities in the application of regulatory requirements. On top of this, there is significant momentum behind the US developing its own framework. Some actors believe the pressure for a global set of standards is rising, though local regulation remains fragmented.

EU and UK models provide the building blocks for a principles-based framework. The EU's GDPR has become a default standard owing to its extraterritorial impact. The requirements outlined in these systems provide a starting point for navigating the evolving requirements in jurisdictions like China, Indonesia, and India. A principles-based framework that is firm centered, flexible, and practical can provide a strong model for firms working across jurisdictions and navigating dynamic regulatory requirements.

Building pathways to trust is critical to practical models. Firms must balance innovative uses for data with increasingly complex protection systems. In that context, compliance is an ongoing process, and firms are seeking to prioritize culture as much as putting in place legally compliant systems in each jurisdiction of operation. Therefore, firms will likely build personalized solutions, based on their desired usage of the data gathered.

We look forward to continuing the DataTalk series in October, when we will discuss developments in the data created and analyzed by the market, and how geopolitical moves shape the information flows.