Briefing Note | **DataTalk** 25

# Data Security: Protecting privacy and preventing data misuse

May 2023

*Protecting customer privacy and providing security for the information held by Financial Institutions (FIs) is one of the main drivers of best practices for data management and innovation in the sector. The May session of DataTalk explored data security in this context. The session covered key topics such as the importance of data flows for customer and business operations, the impact of external forces on data management, and the importance of the role of the industry in building a framework for data security. This briefing note summarizes the discussion held on May 17, 2023, respecting that the forum is conducted under the Chatham House Rule and does not represent the official position of the IIF or its membership.*

**Data security equals customer trust.** FIs and third parties (e.g., cloud service providers, partners from other sectors, etc.) are increasingly inter-reliant to provide the services customers have come to expect. Strong third-party risk management is important to prevent data breaches from occurring so that customer trust in the systems, products, and services can be maintained. The third-party service model is drawing increasingly close attention from regulatory authorities (e.g., Open Data, Embedded Finance, Critical Third Parties, etc.). Nonetheless, FIs of all sizes are evaluating their third-party service providers to ensure compliance, not just with the minimum regulatory standards, but also with the standards expected by the consumers to maintain their trust.

**Data flows are critical to business operations and customer service.** FIs have come to operate with others outside the traditional banking ecosystem. New use cases for encryption and synthetic data to prevent unwanted access, for example, are proving to have transformative potential for improving the protection of information. While the benefits of implementing new technological advances into operational processes are clear, FIs need to balance the benefits of these technologies, their costs, conflicting regulatory requirements, and customers' demands in terms of speed and safety.

**Data classification: enhancing security.** Personally identifiable information is not often in one data source but, in fact, found across multiple sources. This is why knowing the data source and the type of data itself is key to good data management. A risk-based whole-systems approach means first correctly classifying data based on the sensitivity of the information, and then applying security-enhancing techniques depending on the classification (e.g., encryption, access restriction, confidential computing).

**Data localization is impacting FIs' ability to secure data.** Measures for fraud prevention, data resiliency plans, business continuity, access to real-time cross-border transfers, and best practices for data management play a critical role in ensuring data security. Trends toward localization could inhibit FIs from offering sufficient security for their customers, which should be taken into account by national authorities when drafting data regulations.

**FIs have a lot at stake but just as much to offer.** In terms of a regulatory framework for data security, the industry is well-placed to make informed contributions. Therefore, opening collaborative spaces where industry and authorities can exchange their views would have a good impact going forward.

*We look forward to continuing the DataTalk series on Tuesday, June 20 at 9:00 AM Washington DC / 2:00 PM London, where we will explore AI, its governance, the pursuit of ethical AI, and how it interacts with third-party providers.*