PIFS

Program on International Financial Systems

Data Localization, Cloud Adoption, and the Financial Sector

JULY 2024

The Program on International Financial Systems (PIFS) is a 501(c)(3) organization that conducts research on issues impacting the global financial system. PIFS also hosts international symposia, executive education programs and special events that foster dialogue and promote education on these issues. PIFS was founded in 1986, by Hal S. Scott, now Professor Emeritus of Harvard Law School. Over thirty years later, Hal Scott continues to lead PIFS.

This report was prepared by Hal Scott (Chairman and President of PIFS), John Gulliver, (Executive Director), Hillel Nadler (Senior Research Fellow), and Jon Ondrejko (Senior Vice President of Programs).

Amazon Web Services, Inc. is a financial sponsor of PIFS.

Data Localization, Cloud Adoption, and the Financial Sector

JULY 2024

Table of Contents

EXECUTIVE SUMMARY

In an increasingly interconnected world, the ability of financial institutions to move data across borders is critical to their success and ability to serve their customers. Yet, a growing number of jurisdictions are imposing "data localization" requirements that restrict or even prohibit the transfer of data outside their borders. This report examines how these requirements affect the financial sector in light of the growing adoption of cloud computing technology. Data localization requirements, while often motivated by legitimate policy concerns, impose significant costs on financial institutions and their customers, including by preventing financial institutions from harnessing the full potential of cloud computing. Regulators can address those concerns without impeding the free flow of data that is essential to realizing the benefits of cloud adoption in the financial sector.

The Promise of Cloud Technology for the Financial Sector

The COVID-19 pandemic accelerated a trend that was already well underway: the adoption of cloud computing by financial institutions. Cloud technology offers significant benefits, including cost efficiency, enhanced cybersecurity, and operational resilience. By allowing financial institutions to automatically scale up their computing resources, cloud technology enables them to handle market stress events, such as unexpected surges in trading volumes or cyberattacks, that might overwhelm traditional information technology (IT) infrastructure. Moreover, the extensive computing resources available in the cloud facilitate access to cutting-edge technologies like data analytics and artificial intelligence (AI), which promise to transform how financial institutions meet their customers' needs and manage risk.

The Critical Role of Cross-Border Data Flows in Finance

Cross-border data transfers are essential to the global financial sector. They are necessary for processing international payments, providing financial services to customers who live or do business in multiple jurisdictions, and facilitating regulatory oversight. Even local financial institutions rely on cross-border data flows when they connect their customers to global financial networks. By impeding these flows, data localization requirements limit the ability of financial institutions to meet their customers' needs and even the ability of financial regulators to engage in effective oversight.

Data Localization Requirements and Cloud Adoption

Proponents of data localization often argue that it enhances data privacy, ensures data availability in the event of a disruption, and facilitates regulatory oversight and law enforcement. However, these arguments are misguided. The physical location of data is neither necessary nor sufficient for its security; data that is not managed securely can be compromised regardless of where it is stored. Moreover, the major cloud providers, due to economies of scale, can invest far more in cybersecurity and resilience than local technology providers. And local data storage does not guarantee regulatory access; regulators can ensure access to data stored abroad through bilateral or multilateral agreements. Data localization requirements also threaten to cut financial institutions off from the benefits of cloud adoption, which depend critically on the ability to move data across borders.

The major cloud providers do not maintain data centers in every jurisdiction. Instead, they leverage economies of scale by operating a global network of data centers. This distributed infrastructure is key to the cloud's resilience and cybersecurity advantages: data and processes can be spread across different data centers, making them less vulnerable to localized disruptions or attacks. That distributed infrastructure also provides the massive computing resources that enable cutting-edge analytics and AI.

Policy Recommendations for Financial Regulators

To balance legitimate policy concerns with the imperative of facilitating cross-border data flows to enable cloud adoption, the report recommends that financial regulators:

- Adopt a principles-based approach to data protection that focuses on ensuring that data is stored securely, rather than where it is stored.
- Work together with regulated entities and cloud service providers to leverage global, out-of-jurisdiction cloud infrastructure in a manner that enhances cybersecurity and operational resilience.
- Ensure access to data for regulatory supervision and law enforcement through agreements with other jurisdictions, not through data localization.
- Increase coordination with other local authorities and foreign counterparts to develop consistent policies for data transfer.

Conclusion

Data localization requirements, while often based on legitimate concerns, impose significant costs on financial institutions and their customers. They inhibit the ability of financial institutions to leverage cloud technology for enhanced security, resilience, and innovation. By adopting policies that facilitate secure cross-border data flows, financial regulators can address their legitimate concerns without hampering the global financial sector. In an increasingly interconnected world, the free flow of data is not just beneficial; it is essential.

INTRODUCTION

The financial sector runs on information: the success of financial institutions depends on their ability to obtain, protect, and use information for their benefit and the benefit of their customers. Financial data includes information about customers such as their name and account number and information about companies and their key employees. The increasing reliance by financial institutions on cloud services to securely and efficiently store, process, and transmit information has raised challenges for how jurisdictions regulate financial data.

In a global market, like the market for financial services, the free flow of data across borders generates significant value. The cross-border movement of data is essential to processing international payments, providing financial services to individual and business customers, and improving risk management at the financial institution level. Yet recent years have seen the imposition of "data localization" requirements: restrictions which directly require, or have, as a consequence, that data originating in a jurisdiction remain in that jurisdiction.[1]

This report analyzes data localization requirements and their impact on the financial sector. Part I of the report provides background on cloud adoption in the financial sector and the critical role of cross-border data flows to the financial sector. Part II takes a deeper dive into the different kinds of data localization requirements, the stated motivations for adopting data localization requirements, and their potential drawbacks. Part III focuses on how data localization requirements affect financial institutions and their ability to benefit from cloud adoption.

Part IV concludes with policy recommendations for financial regulators regarding cross-border data transfer in the context of cloud adoption that address the concerns that national governments and financial regulators have used to justify data localization requirements. Regulators should take a principles-based approach to data protection that allows secure data transfer to other jurisdictions, as long as they afford sufficient levels of protection to private data. They must also recognize that global, out-of-jurisdiction technology infrastructure can enhance cybersecurity and operational resilience. Rather than focusing on the *location* of data, regulators can address concerns about regulatory oversight and law enforcement by ensuring *access* to data. In addition, they should work to align data transfer policies with other local authorities and regulators in other jurisdictions.

[1] David McCabe and Adam Satariano, *The Era of Borderless Data Is Ending*, NEW YORK TIMES (May 23, 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html.

PART I: CLOUD ADOPTION AND INTERNATIONAL DATA TRANSFERS IN THE FINANCIAL SECTOR

Cloud computing allows data to be stored on remote servers maintained by a third-party provider and retrieved over a network, such as the internet, rather than on proprietary, on-premises infrastructure.[2] Although cloud computing is not new to the financial sector, the COVID-19 pandemic accelerated cloud adoption by financial institutions. Cloud adoption holds significant promise for cost efficiency, operational resiliency, cybersecurity, and innovation by financial institutions. It also helps facilitate secure cross-border data flows, which play a critical role in the global financial services market. However, data localization requirements impair the ability of financial institutions to leverage cloud technology for their benefits and the benefit of their customers.

a. Cloud adoption in the financial sector

Financial institutions have been using cloud technology, in one form or another, for almost two decades.[3] The adoption of cloud services in the financial sector was thus already underway before the COVID-19 pandemic.[4] The pandemic accelerated the demand for cloud services, as financial institutions were forced to move away from in-person customer service and support a remote workforce. Cloud adoption enabled financial institutions to scale up remote services in a matter of days.[5]

According to a recent survey of global financial institutions, 98 percent of respondents maintained at least some data, applications, or operations in the cloud.[6] Banco Santander, one of the world's largest banks, plans to migrate most of its core banking services to the cloud by the end of 2024.[7] Latin America's largest bank, Itau Unibanco, will move a majority of its systems to the cloud over a ten-year period. [8] Some banks have gone even further: Capital One, one of the largest banks in the United States, announced in 2021 that it had shuttered its private data centers and had transitioned all of its core services to the cloud.[9] Other financial institutions—including investment companies, broker-dealers, investment advisors, and insurance companies—have also migrated some

[2] Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Sep. 2011), https://csrc.nist.gov/pubs/sp/800/145/final.
[3] Lisa Valentine, *Clouded outlook*, 104 ABA BANKING JOURNAL 22 (Sep. 2012).
[4] Jerry Silva, *Banking on the Cloud: Results from the 2020 CloudPath Survey*, IDC PERSPECTIVE 7-8 (Nov. 2020).
[5] Daniel Pujazon and Brad Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, INSTITUTE OF INTERNATIONAL FINANCE 4-5 (Jun., 2020), https://www.iif.com/portals/0/Files/content/32370132_iif_cloud_computing_resilience.pdf.
[6] CLOUD SECURITY ALLIANCE, *State of Financial Services in Cloud* (2023). Respondents included banks and credit unions, fintechs, and other financial institutions in the Americas (52%), EMEA (28%) and the Asia-Pacific (20%) regions.
[7] BANCO SANTANDER, *Santander passes key milestone in its transformation after migrating its CIB banking platform to the cloud* (Dec. 11, 2023), https://www.santander.com/en/press-room/press-releases/2023/12/santander-passes-key-milestone-in-its-transformation-after-migrating-its-cib-banking-platform-to-the-cloud.
[8] Samantha Lipana and Marissa Ramos, *Latin America's 30 largest banks by assets, 2024*, S&P GLOBAL MARKET INTELLIGENCE (Apr. 30, 2024), https://www.spglobal.com/marketintelligence/en/news-insights/research/latin-americas-30-largest-banks-by-assets-2024.
[9] Adrian Jimenea et al., *The world's largest banks by assets, 2024*, S&P GLOBAL MARKET INTELLIGENCE (Apr. 30, 2024), https://www.spglobal.com/marketintelligence/en/news-insights/research/the-worlds-largest-banks-by-assets-2024; Lananh Nguyen, *Banks Tiptoe Toward Their Cloud-Based Future*, NEW YORK TIMES (Jan. 3, 2022), https://www.nytimes.com/2022/01/03/business/wall-street-cloud-computing.html.

operations to the cloud.[10] And several financial market utilities, including clearinghouses and exchanges, have transitioned to the cloud in some capacity.[11]

Although financial institutions like Banco Santander and Capital One have gone all-in (or close to it) on cloud computing, adoption in the financial sector is still in its early stages. The same industry survey that reported 98 percent cloud adoption also reported that nearly half of respondents maintain less than ten percent of their business-critical workloads in the cloud. Similarly, almost half of the respondents report that less than ten percent of their regulated workloads have been migrated to public cloud environments.[12] Financial institutions have mostly used the cloud for enterprise applications like human resources and collaboration tools. Most core operations are still mostly conducted using legacy IT systems.[13]

b. The benefits of cloud technology for financial institutions—and their customers

Still, cloud adoption in the financial sector—including for core operations—is expected to increase in the coming years. The cloud model, which makes computing resources available on demand and allows customers to only pay for resources they actually use, allows financial institutions to turn large, up-front IT expenditures into smaller, ongoing operational costs.[14] According to some estimates, cloud adoption can reduce IT costs by between 20 and 50 percent, amounting to hundreds of millions of dollars of cost savings economy-wide.[15] Transforming large capital expenditures into ongoing operational costs also makes financial institutions more technologically agile: they can test new scenarios, software tools and alternative configurations without a lengthy purchasing and provisioning process. Lower costs and greater technological agility translate into better products and services for customers, especially digital financial products with robust features and data. Cloud computing also levels the technological playing field between financial institutions of different sizes, by giving smaller institutions and fintech startups access to computing resources that were previously only available to larger institutions with the ability to devote significant resources to technology infrastructure.[16]

---

[10] Amazon Web Services, *Vanguard Increases Investor Value Using Amazon ECS and AWS Fargate* (2021), https://aws.amazon.com/solutions/case-studies/vanguard-ecs-fargate-case-study/.

[11] CME Group, *CME Group Signs 10-Year Partnership with Google Cloud to Transform Global Derivatives Markets Through Cloud Adoption* (Nov. 4, 2021), https://www.cmegroup.com/media-room/press-releases/2021/11/04/cme_group_signs_10-yearpartnershipwithgooglecloudtotransformglob.html; Nasdaq, *Nasdaq and AWS Partner to Transform Capital Markets* (Nov. 30, 2021), https://www.nasdaq.com/press-release/nasdaq-and-aws-partner-to-transform-capital-markets-2021-12-01; New York Stock Exchange, *NYSE Market Data via Amazon Web Services (AWS),* https://www.nyse.com/nyse-cloud.

[12] Cloud Security Alliance, *State of Financial Services in Cloud* (2023).

[13] Id.

[14] Depository Trust & Clearing Corporation, *Moving Financial Market Infrastructure to the Cloud*, 5-6 (May 2017).

[15] Patrick Wauters, et al., *Measuring the economic impact of cloud computing in Europe,* Deloitte (2016), https://ec.europa.eu/newsroom/dae/redirection/document/41184.

[16] Wang Jin and Kristina McElheran, *Economies before Scale: IT Strategy and Performance Dynamics of Young US Businesses*, Rotman School of Management Working Paper No. 3112901 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112901. Cloud providers can enable compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) by offering a secure environment for storing, processing, and transmitting credit card information. See generally, Cloud Special Interest Group and Payment Card Industry Security Standards Council, *PCI SSC Cloud Computing Guidelines* (Apr., 2018), https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

By facilitating low-cost innovation and increased competition, cloud migration helps expand financial access and inclusion, particularly for customers in developing or underserved markets.[17] At the global level, the share of adults with an account at a financial institution or mobile money service increased from 51 to 76 percent over the decade spanning 2011 to 2021.[18] Cloud-based financial platforms have played a critical role in reaching previously underserved businesses and individuals. In China, for example, WeBank's cloud-native approach has allowed its lending platform to reach millions of individuals and businesses with little to no credit history.[19] Nubank, a Brazilian mobile-only bank, uses cloud-based infrastructure to offer credit cards and personal loans to customers who could not get loans from traditional banks due to their lack of credit history.[20] In Southeast Asia, ride-hailing apps such as Grab and Go-Jek (now GoTo) have leveraged cloud infrastructure to provide payments and other financial services to retail users.[21] Mercado Libre, the largest online commerce and payments provider in Latin America, offers cloud-based payment and credit services to customers who would otherwise lack access to them.[22]

Cloud computing can also be more secure and resilient than traditional infrastructure. Unlike all but the largest financial institutions, the major cloud providers are at the forefront of security research and implementation.[23] The platforms of the major cloud providers are also built to give customers tools to implement stringent security requirements, such as monitoring and logging for all activities and built-in data encryption.[24] The scalability of cloud services allows financial institutions to handle unexpected capacity requirements—whether due to an unanticipated surge in market activity or a malicious cyberattack—that might overwhelm a financial institution's own IT infrastructure.[25] Moreover, since cloud infrastructure is more geographically distributed across data centers and regions than

[17] World Bank and the International Monetary Fund, Bali Fintech Agenda (2018); Max Chuard, *Cloud and SaaS technology can drive inclusive banking. Here are 3 reasons how*, World Economic Forum (Dec. 10, 2020), https://www.weforum.org/agenda/2020/12/cloud-and-saas-technology-can-drive-inclusive-banking/.

[18] World Bank, *The Global Findex Database: Measuring Financial Inclusion and the Fintech Revolution* (2024), https://www.worldbank.org/en/publication/globalfindex.

[19] Sally Chen et al., *Virtual Banking and Beyond*, 120 BIS Papers (Jan. 2022), https://www.bis.org/publ/bppdf/bispap120.pdf.

[20] Debopriyo Bhattacharyya et al., *Global Banking Annual Review 2023: The Great Banking Transition*, McKinsey & Company (Oct. 10, 2023), https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review.

[21] Grab, *Grab forges strategic cloud partnership with Microsoft to drive innovation and adoption of digital services across Southeast Asia* (Oct. 9, 2018), https://www.grab.com/sg/press/business/grab-forges-strategic-cloud-partnership-with-microsoft-to-drive-innovation-and-adoption-of-digital-services-across-southeast-asia/; Leon Spencer, *Indonesia's GoTo Group goes with Google Cloud for next phase of Asian attack*, Channel Asia (Jul. 27, 2021), https://www.channelasia.tech/article/1269704/indonesias-goto-group-goes-with-google-cloud-for-next-phase-of-asian-attack-2.html.

[22] Frost et al., *BigTech and the changing structure of financial intermediation*, 34(100) Economic Policy 761-799 (2019).

[23] The major cloud providers, for example, detected and quickly mitigated significant chip-level security vulnerabilities that had been discovered by one of the providers. Jordan Novet, *Amazon, Microsoft, and Google respond to Intel chip vulnerability*, CNBC (Jan. 3, 2018), https://www.cnbc.com/2018/01/03/microsoft-google-respond-to-intel-chip-vulnerability.html.

[24] Depository Trust & Clearing Corporation, *Moving Financial Market Infrastructure to the Cloud* (May 2017).

[25] Amazon Web Services, *AWS Best Practices for DDoS Resiliency*, 6-15 (2021), https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf.

traditional IT infrastructure, cloud adoption facilitates greater resiliency in the event of a local outage.[26]

The extensive computing resources and automatic scalability of the cloud also makes it uniquely suited to transforming how financial institutions handle data. Cloud-based environments enable financial institutions to ingest data at far greater speeds than are available with traditional IT infrastructure. They also facilitate unprecedented analysis and manipulation of data once they are ingested.[27] That sophisticated level of data analysis can help financial institutions gain competitive advantages, improve their risk management, and enhance existing functions such as fraud and money laundering detection. Recent breakthroughs in the training and deployment of large language models and other machine learning and AI tools would have been impossible without the massive computing resources available in cloud environments.[28] Any financial institution that seeks to leverage machine learning or AI in the future will need to rely on cloud infrastructure.

c. The importance of cross-border data flows in the global financial services sector

In the financial sector, data is an essential asset that facilitates informed financial decisions. In an increasingly globalized financial services market, the secure flow of data across borders is critical for financial institutions to succeed. For example, a financial institution that operates branches or affiliates in multiple jurisdictions might want to share information regarding its customers in one jurisdiction with an affiliate in another jurisdiction in order to serve a client that has moved from one jurisdiction to another.[29] Financial institutions benefit from market analysis or due diligence activities in which the transfer of data across borders is of material importance.[30] And financial institutions may rely on the international transfer of consumer or business credit data for creditworthiness determinations.[31]

More fundamentally, transactions that are vital to the international financial system, including cross-border payment systems, rely on the international flow of data.[32] As international mobility in goods, services, capital and people has increased over time, the importance of the cross-border transactions has grown in both volume and value.[33] In 2022,

---

[26] Depository Trust & Clearing Corporation, *Moving Financial Market Infrastructure to the Cloud* (May 2017). See also Glen Robinson et al., *Using Amazon Web Services for Disaster Recovery*, Amazon Web Services (October 2014), https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.121b65092f931567af5370b47dd12cb18866089c.pdf.

[27] Davies, New *Tools Give Better Picture, Literally, of Financial-System Risk*, Wall Street Journal (2017), https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk1493086260?mod=article_inline; John Ashley and Jochen Papenbrock, *Modern Computing Platforms as Key Technology for Central Banks, Financial Supervisors, and Regulators*, Irving Fisher Committee on Central Bank Statistics (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, Global Economy and Development (Mar. 2018).

[28] Id.

[29] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press (1998).

[30] Id.

[31] Id.

[32] Id.; Bank of England, *Cross-border Payments* (Jan. 31, 2023), https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments.

[33] Bank of England, *Working together to enhance cross-border payments - speech by Victoria Cleland* (Nov. 22, 2021), https://www.bankofengland.co.uk/speech/2021/november/victoria-cleland-keynote-presentation-the-cbpc-international-payments-on-the-move.

annual cross-border payments reached approximately $150 trillion.[34] And over the course of 2023, outstanding cross-border financial claims increased by more than $2 trillion.[35]

The advent and widespread adoption of cloud technology has created new opportunities for financial institutions to benefit from cross-border data flows. Although the major cloud providers' infrastructure is widely distributed across geographic regions, they do not maintain data centers in every jurisdiction.[36] To exploit the benefits of cloud technology, financial institutions may have to transfer data to another jurisdiction. For example, recent high-profile advances in the fields of data analytics and AI hold out significant promise for the financial sector. Multinational banks collect detailed information about how their customers behave, and use big data analytics or AI to develop tailored services such as personalized alerts and better fraud detection.[37] These fields depend on processing massive volumes of data for training and producing useful insights, which requires access to computing resources which are only available from the largest cloud providers, and which may not be located in a financial institution's home jurisdiction.[38]

Restrictions on cross-border data transfers, which have increased significantly in recent years, therefore hamper financial institutions' capacity to compete in, and take advantage of, the global financial services market. Data localization requirements limit their ability to best serve their customers. And if they limit their opportunities to leverage cloud technology, those requirements impede their access to technologies—like data analysis and AI—that promise to transform the financial sector. It is therefore critical that regulators, including financial regulators, weigh the justifications for restrictions on the cross-border transfer of financial data against their significant costs.

PART II: UNDERSTANDING DATA LOCALIZATION REQUIREMENTS

For as long as firms have used technology to transfer data across borders, regulators have imposed rules governing how they can do so. As the international flow of data has increased, so have efforts to regulate it. Restrictions on the transfer of data out of the originating jurisdiction take different forms, ranging from rules that require that data be physically located where it originates to "de facto" local storage requirements that impose stringent conditions on transferring data out of jurisdiction. Regulators have cited several grounds for imposing data localization requirements, including privacy, economic development, regulatory enforcement, and geopolitical concerns. Data localization

[34] Luca Bionducci et al., *On the cusp of the next payments era: Future opportunities for banks*, MCKINSEY & COMPANY (Sep. 18, 2023), https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report#/.
[35] BANK FOR INTERNATIONAL SETTLEMENTS, *Locational banking statistics, BIS WS_LBS_D_PUB 1.0 (data set)* (2024), https://data.bis.org/topics/LBS/BIS%2CWS_LBS_D_PUB%2C1.0/Q.S.C.A.TO1.A.5J.A.5A.A.5J.N?view=observations.
[36] Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[37] Id.
[38] John Ashley and Jochen Papenbrock, *Modern Computing Platforms as Key Technology for Central Banks, Financial Supervisors, and Regulators*, IRVING FISHER COMMITTEE ON CENTRAL BANK STATISTICS (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, GLOBAL ECONOMY AND DEVELOPMENT (Mar. 2018).

requirements, however, have significant conceptual and practical drawbacks, underscoring the importance of achieving these goals in other ways.

a. Different kinds of data localization requirements

Data localization requirements long predate the cloud. The first national data protection laws, introduced in the late 1970s and early 1980s, required either the localization of data processing operations or prior authorization for the export of sensitive data.[39] Over the past decade, however, as technologies like cloud computing have transformed how data is stored, processed, and shared, restrictions on the cross-border transfer of data have proliferated.[40] According to one study, the number of countries imposing restrictions on the cross-border flow of data almost doubled between 2017 and 2021.[41]

These restrictions vary by country in terms of both their scope and how they limit cross-border data transfers. Some restrictions apply to any data that has been generated within a country; and others apply only to certain categories of data, like financial data, or specific economic sectors or entities. In some jurisdictions, for instance, financial regulators have imposed data localization requirements on financial institutions in the absence of any general restrictions on data transfer in those jurisdictions.[42]

With respect to content, data localization requirements can be divided into three broad categories: (1) explicit local data storage or processing rules, which mandate that data originating in a country be stored or processed in that jurisdiction; (2) "data mirroring" rules, which allow data to be transferred abroad as long as a copy of that data is stored locally; and (3) rules that place conditional restrictions on the transfer of data abroad. Depending on the stringency of those conditions, when the cost of compliance is prohibitive, they amount to de facto local storage requirements.

Local-only data storage or processing rules are the most stringent form of data localization requirement. The People's Republic of China, for example, requires that "critical information infrastructure operators" must store locally in Mainland China such personal information and other "important data" that are collected and generated in China (although data can be transferred abroad under some circumstances). [43] More stringent restrictions apply to financial data: the People's Bank of China mandates that virtually all personal data collected as part of the provision of financial services be stored, processed and analyzed in Mainland China.[44] Turkey mandates that a wide variety of firms and organizations—including publicly traded companies, pension funds, banks, and financial market regulators and infrastructures—locate their live and backup IT systems within the country.[45] Other jurisdictions impose data localization requirements on specific types of entities

[39] Christopher J. Millard, *Legal Protection of Computer Programs and Data*, 14(1-2) INTERNATIONAL JOURNAL OF LEGAL INFORMATION 74-75 (1985).
[40] EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, *Restrictions on Cross-Border Data Flows: A Taxonomy* (2017); INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (2021).
[41] Id.
[42] Javier López González, Francesca Casalini and Juan Porras, *A Preliminary Mapping of Data Localisation Measures*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT TRADE POLICY PAPERS, NO. 262 (2022), https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.
[43] Cybersecurity Law, Article 37; Personal Information Protection Law.
[44] Article 6, Notice No. 17 (2011).
[45] CAPITAL MARKETS BOARD, *Communique on the Management of Information Systems*, VII-128.9 (2018) (publicly traded companies and financial markets regulators and infrastructures); BANKING REGULATORY AND SUPERVISORY AUTHORITY, *Regulation on Information Systems and Electronic Banking Services of Banks* (2020) (banks).

or infrastructure: Venezuela, for example, requires that technology infrastructure for payment processing be located domestically.[46] And the Central Bank of Nigeria requires that domestic payment transactions, including point-of-sale and ATM transactions, be routed domestically for switching between Nigerian issuers and acquirers.[47]

"Data mirroring" requirements are less restrictive than local-only data storage rules, since they only mandate that a copy of data be kept on local servers or data centers, to ensure operational resilience in case of an outage or other disruption. That means that data can be transferred and processed abroad, as long as a copy of the data is kept locally. However, the requirement that a redundant copy of data be kept locally raises the relative cost of storing data abroad, and thus in practice may have the same effect as local-only storage rules.[48] Mexico requires certain financial institutions, such as banks and fintech firms, that store data in data centers located outside of Mexico to maintain copies of accounting and transactional records locally to ensure operational continuity.[49] Likewise, Chile mandates that banks that outsource critical workloads abroad, including through the use of cloud services, maintain a local data processing center for contingency purposes.[50]

Other jurisdictions impose conditional restrictions on international data transfers. These conditional restrictions take on a variety of different forms. Some countries mandate that data only be transferred to another jurisdiction that has in place equivalent data protection rules or data protection is ensured by contract. For example, Brazil's data protection law only allows international transfers of personal data where the recipient country provides an "adequate" level of data protection or where certain contractual provisions are in place.[51] Other jurisdictions require that companies obtain the consent of regulators or customers before transferring data abroad. Saudi Arabia, for example, requires that personal data be stored and processed locally unless written approval has been obtained from the relevant regulatory authority.[52] Panama's bank and capital markets regulators, for example, requires that regulated entities obtain prior approval for the use of foreign cloud services provided by a third party.[53] Mexican financial institutions are subject to similar requirements.[54]

b. Reasons for data localization requirements

There are a wide variety of motivations for data localization policies. One commonly stated concern is that data transferred abroad, especially sensitive personal data like financial data, is not adequately safeguarded against potential security breaches or foreign government access.[55] Alternatively, regulators worry that data stored abroad will not be

[46] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (Jul. 2021).
[47] CENTRAL BANK OF NIGERIA, *Guidelines on Point of Sale Card Acceptance Services* 4.4.8.
[48] Id.
[49] Electronic payment funds institutions (Fintechs), Article 49, IV; Banks (Annex 52(I)(e)); Brokerage houses, Annex 12(I)(e). In addition, Mexican financial institutions that use cloud services can only connect to the Interbank Electronic Payment System (SPEI) using local data centers.
[50] Circular Banking 2409/Financial 798 Chapter 20-7. Banks can only outsource data processing services to jurisdictions that have an investment grade country risk rating and adequate legal protection for the security of personal data.
[51] Law on General Data Protection, Chapter V – International Data Transfer. See also Peru's draft regulation on data protection.
[52] National Data Governance Interim Regulations, Section 5.4 (2020).
[53] Acuerdo No. 003-2012; Acuerdo No. 005-2018.
[54] See, e.g., Electronic payment funds institutions (Fintechs), Article 49, VIII.
[55] Christopher Millard, *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, CLOUD AND THE LAW (2015).

available in the event of a disruption.[56] Local data storage, the argument goes, is necessary to protect data against unwanted intrusions and unanticipated disruptions.

In addition to purported privacy and availability concerns, countries connect data localization requirements with the broad concept of "digital sovereignty." In the European context, digital sovereignty has been defined as the "ability to act independently in the digital world," in relation to "both protective mechanisms and offensive tools to foster digital innovation."[57]

Accordingly, some countries have justified data localization requirements on the ground that direct access to companies can facilitate the enforcement of laws, such as tax and anti-money laundering statutes.[58] When data is located abroad, legal authorities worry that their ability to access data may be hampered. This argument is particularly relevant for sectors, like the financial services sector, that are subject to disclosure requirements and maintain data that is highly sought after by law enforcement authorities. Local storage of data might facilitate surveillance and other involuntary disclosures of information by regulated entities. However, this rationale arguably undercuts the privacy rationale for data localization.[59]

Countries also introduce data localization requirements with the goal of incentivizing investment in their local information technology sectors, another aim connected with the notion of digital sovereignty. If companies are required to store and process data locally, they will be forced to invest in local servers and data centers. That investment, in theory, could create spillover benefits for the local high-tech sector.[60] Beyond the economic benefits of domestic investment in technology infrastructure like data centers, some governments view local data processing centers as critical infrastructure necessary to their national security and sovereignty.[61] In addition, the disruption of certain critical services, like financial services, could severely impair the country's basic functioning, which warrants special requirements to ensure the resilience and availability of those services.[62]

c. Costs of data localization generally

While these policy aims are legitimate (if potentially contradictory), the use of data localization requirements to achieve them is likely to be ineffective. The physical location of data may be one factor in its privacy, but it is not the most important. From a technical perspective, physical access to a server or other data storage device is neither necessary nor sufficient for access to the information stored on it. Data that is not managed securely

---

[56] Id.
[57] European Parliamentary Research Service, *Digital sovereignty for Europe* (Jul., 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.
[58] Institute of International Finance, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (Mar. 2019).
[59] Christopher Millard, *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, Cloud and the Law (2015).
[60] Institute of International Finance, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (Mar. 2019).
[61] Center for Strategic and International Studies, *The Real National Security Concerns over Data Localization* (2021); Association for Financial Markets in Europe, *European Cybersecurity Certification Scheme for Cloud Services (EUCS) – Solutions on the Issue of Independence to Non-EU Law* (March 13, 2023), https://www.afme.eu/Portals/0/DispatchFeaturedImages/230310_AFME%20Comments%20on%20EUCS_FINAL.pdf; International Organization of Securities Commissions, *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (May 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.
[62] Id.

can be accessed even if a user lacks physical access to a server. And if data are securely encrypted, physical access alone won't make it accessible in an intelligible form. Moreover, if data are securely encrypted, physical access to data will not give rise to privacy risks regardless of where they are physically stored.[63]

Local data storage does not necessarily improve the security or availability of data. Storage of data using the foreign infrastructure of a major cloud provider can offer improved security and availability. Economies of scale allow major cloud providers make investments in resilience and cybersecurity capabilities that far exceed those available with local technology infrastructure alone.[64] In addition, the major cloud providers ensure data security and availability by distributing data and processes among multiple systems and locations, making them less vulnerable to a breach or disruption.[65] By mandating that data remain in a particular jurisdiction, localization requirements inhibit the use of that distributed infrastructure. Moreover, by increasing the number and locations of data centers that must be staffed and maintained by companies that operate in different jurisdictions, data localization requirements also add risk and complexity to their cybersecurity operations. Requiring any multinational company to create and defend multiple versions of its systems across different locales means more hardware, more employees, and more vendors, increasing the surface area for potential disruptions or cyberattacks.[66]

Mandating local data storage also does not eliminate the risk of foreign government access. U.S. law, for example, provides that cloud service providers subject to U.S. jurisdiction cannot avoid compliance with an access request from law enforcement authorities simply because data is located in a non-U.S. jurisdiction.[67] Nor does local data storage ensure local regulatory supervision or access for local law enforcement. U.S.-based cloud service providers, for instance, are generally barred from sharing data with foreign governments, regardless of where the data is located. From the perspective of U.S. law, it does not matter whether the data is stored in a U.S. data center or one located in another country. The best way for regulators and enforcement authorities to ensure access to data is not localization, but through bilateral or multilateral data sharing agreements. Some jurisdictions have worked with foreign governments to facilitate access to their own citizens' data stored abroad. Several countries, for instance, have entered into bilateral agreements with the United States so that U.S. cloud providers can comply with lawful requests for electronic data issued by the other country without a warrant directly to the cloud provider.[68]

Even if data localization may offer some direct economic benefits, those benefits are limited. Although data localization can attract investment in domestic technology infrastructure, such as data centers, the spillover benefits are minimal because data centers are highly automated and have relatively few permanent employees.[69] More fundamentally,

[63] Christopher Millard, *Cloud Computing Law*, OXFORD UNIVERSITY PRESS (2013).
[64] See above, Part I.b.
[65] Id.
[66] Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 JOURNAL OF INTERNATIONAL ECONOMIC LAW 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626; BLANCCO, *The High Cost of Cluttered Data Centers* (2019).
[67] CLOUD Act.
[68] Id.
[69] Nigel Cory, *The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (Apr. 2019).

competition over the location of the major cloud providers' infrastructure is a zero-sum game: it is not economically feasible for cloud providers to build data centers, costing hundreds of millions of dollars or more,[70] in *every* jurisdiction. Major cloud providers may choose instead not to build out local infrastructure. In that case, data localization requirements will harm the local economy, by cutting domestic businesses off from the benefits offered by major cloud providers' best-in-class technology infrastructure. That translates into higher technology costs: according to one study, data localization requirements can increase the costs of data hosting by 30-60 percent.[71] Increased costs mean reducing local companies' ability to compete on a global scale and less innovation for local customers. Moreover, increases in the restrictiveness of a country's data transfer rules have been linked to meaningful decreases in productivity and increases in price in affected industries.[72]

Some jurisdictions have recognized that the confidentiality, integrity and availability of data can best be achieved through the use of cloud servers located abroad.[73] Estonia, for example, has established a virtual "data embassy" using foreign cloud services to ensure the continuity of data that is deemed critical to the functioning of the state. Other governments have revised existing data localization requirements in light of the costs associated with them. Indonesia, for example, narrowed its strict data localization requirements, which previously applied to any provider of electronic "public services," to only apply to government entities.[74] And Ukraine lifted data localization requirements in order to transfer critical government and private sector data, including the data at its largest private bank, to secure foreign cloud servers before Russia's invasion.[75]

PART III: DATA LOCALIZATION REQUIREMENTS AND THE FINANCIAL SECTOR

The proliferation of data localization requirements, which impede the flow of data across borders, raises particular issues for financial services. The cross-border transfer of data within multinational entities, and between entities in different jurisdictions, is critical to the operation of the global financial sector. The largest financial institutions rely on the free

[70] Matt Vincent, *Hyperscale Cloud Giants' Data Center Mega Deals Keep Sprouting Zeroes*, DATA CENTER FRONTIER (Apr. 1, 2024), https://www.datacenterfrontier.com/hyperscale/article/55001427/hyperscale-cloud-giants-data-center-mega-deals-keep-sprouting-zeroes; AMAZON WEB SERVICES, AWS to Launch an Infrastructure Region in Mexico (Feb. 26, 2024), https://press.aboutamazon.com/2024/2/aws-to-launch-an-infrastructure-region-in-mexico.

[71] LEVIATHAN SECURITY GROUP, *Quantifying the Cost of Forced Localization* (2015), https://static1.squarespace.com/static/6128b1eb2eb2cf15b7a35a2f/t/65af6b484ec970386fd56386/1705995081389/Quantifying%2Bthe%2BCost%2Bof%2BForced%2BLocalization.pdf.

[72] INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (2021); EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (2014); Martina F. Ferracane, *The Costs of Data Protectionism*, BIG DATA AND GLOBAL TRADE LAW (Jul. 9, 2021). Cloud adoption has also been linked to emissions reductions, as data center activity is moved from less efficient on-premises servers to newer, more efficient public cloud servers. FTI CONSULTING, *Economic Impact of Cloud Adoption in Six Latin American Countries* (Oct. 20, 2023), https://fticommunications.com/economic-impact-of-cloud-adoption-in-six-latin-american-countries/?utm_source=web_linkedin&utm_medium=aws_social&utm_campaign=latam_awr_cloud_adoption_economic_impact_10-25-2023&utm_content=aws-cloud-adoption-economic-impact-report.

[73] E-ESTONIA, *e-Governance*, https://e-estonia.com/solutions/e-governance/data-embassy/.

[74] Government Regulation No. 71 (2019).

[75] Ryan White, *How the cloud saved Ukraine's data from Russian attacks*, C4ISRNET (Jun. 22, 2022), https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/; David E. Sanger, *New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms*, NEW YORK TIMES (Mar. 2, 2023), https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

flow of data to operate seamlessly in different jurisdictions across the globe. And smaller, local financial institutions rely on those larger institutions to provide international services to their own clients, who—in a world where global commerce is the norm—can require financial services where the local institution does not operate.

A French citizen vacationing in the Dominican Republic may need to take out money using a local ATM machine; or a Peruvian vendor selling goods in the Japan over the internet may want to receive payment in a foreign currency. In either case, the transaction can only be processed, and the money transferred, if data moves across international borders. Authorization for the ATM withdrawal must come from a computer system in France, which requires transfer of the customer's data abroad. The online sale involves the transfer of both the customer's and vendor's data between banks and payment processors located in both jurisdictions.

These are only a couple of the ways in which cross-border data flows are critical to the operation of the financial sector. Data localization requirements limit the ability of financial institutions to operate across borders, inhibiting their ability to meet the needs of their customers and even the ability of financial regulators to engage in oversight. They also prevent financial institutions from taking advantage of new opportunities, such as large-scale data analysis and AI, afforded by cloud technology.

a. Complex data regulations increase costs and stifle competition

In addition to their substantive restrictions on cross-border data transfer, data localization rules can also be difficult to implement and comply with. For one, there can be considerable uncertainty about the scope of data privacy rules. It can be unclear which entities are subject to them and to what data they apply.[76] Although data localization rules often distinguish between personal and non-personal data, the line between them is not always clear.[77] Information about particular individuals like key employees (personal data) is sometimes embedded in information about companies (non-personal data).[78] In addition, sophisticated data analysis tools make it easier than ever to infer personal information from purportedly non-personal data.[79] As a result, localization requirements that ostensibly apply only to personal data can in practice limit the transfer of all data, whether personal or not. Another source of complexity is that financial institutions may be subject to specific data localization rules that supplement general data protection laws in a particular jurisdiction.[80] The combination of general data protection rules with specific rules applicable to financial services can give rise to significant compliance costs.

[76] Dmitry Kurochkin, Marat Agabalyan and Saglara Ildzhirinova, *Russia's New Server Localization Law: Implications for Foreign Companies*, BLOOMBERG BNA WORLD DATA PROTECTION REPORT (Feb. 2015), https://news.bloomberglaw.com/privacy-and-data-security/russias-new-server-localization-law-implications-for-foreign-companies.
[77] Michèle Finck and Frank Pallas, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR*, 10(1) INTERNATIONAL DATA PRIVACY LAW 11-36 (Feb. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.
[78] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, BROOKINGS INSTITUTION PRESS (1998).
[79] Michèle Finck and Frank Pallas, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR*, 10(1) INTERNATIONAL DATA PRIVACY LAW 11-36 (Feb. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.
[80] See above, Part II.a.

Consider a global financial institution that is weighing the question of whether to open a branch or affiliate in a jurisdiction that requires local storage (or copies) of certain data. In order to open the branch, the financial institution would have to implement an operational workaround, such as the use of a local software provider or data center for processing and storing data in that jurisdiction. Establishing and maintaining this local solution will require time and money, both operationally and in terms of ensuring compliance with applicable data localization requirements.[81] Those additional costs will be passed on to the financial institution's local customers, leaving them worse off than its customers in other jurisdictions.

Alternatively, the financial institution may decide that the cost of establishing a local workaround is prohibitive and forego the branch or affiliate entirely.[82] Even if the cost of the local solution does not rule it out, the financial institution may find that there is no local solution that meets its own standards—or standards imposed by its home country—for data security or resiliency.[83] Or the financial institution may decide that it is too complicated to develop compliance and risk management policies that are tailored to the specific requirements of that jurisdictions.[84] For any of these reasons, data localization requirements may effectively exclude the financial institutions from the local market, stifling competition and depriving residents of that jurisdiction from access to important services.[85]

Data localization requirements may also inhibit the ability of local financial institutions to serve customers that travel or live abroad. Restrictions on the cross-border transfer of data can make it more difficult to consolidate and analyze customer data from different locations, which is critical for risk management, fraud detection, and customer analytics. If customer data cannot be easily shared or integrated across borders, local financial institutions will face challenges serving their customers in other jurisdictions. Localization requirements can also prevent financial institutions from leveraging global technology infrastructure, limiting their ability to offer consistent and efficient services to customers abroad.[86]

b. Data localization can compromise cybersecurity and resilience

Proponents of data localization requirements frequently appeal to the purported enhancement of cybersecurity and operational resilience. These arguments in favor of data localization are misguided. As noted above, global cloud providers benefit from economies of scale that enable them to make substantially larger investments in data security and availability compared to local or regional infrastructure providers.[87]

---

[81] See, e.g., Prasad, *Mastercard Begins Deleting Indian Transactions Data Stored Overseas* (2019).
[82] Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[83] TechRadar Pro, *The high costs of storing data locally in a cloud native era*, TECHRADAR (Feb. 22, 2019), https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.
[84] INTERNATIONAL REGULATORY STRATEGY GROUP, *How the Trend Towards Data Localisation is Impacting the Financial Services Sector* (Dec. 2020).
[85] Margaret Doyle et al., *How to flourish in an uncertain future: Open banking and PSD2* (2017), https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf.
[86] Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[87] See above, Part I.b.

The distributed nature of storage and processing in the cloud, as well as the greater computing resources available to the major cloud providers compared to individual financial institutions or local technology providers, translate to greater operational resilience. Cloud providers allow a financial institution to automatically scale up and maintain availability in the face of a cyberattack that would overwhelm locally available technology infrastructure.[88] Likewise, by enabling financial institutions to distribute processes and data across different data centers, the cloud enable them to build applications that are online constantly, even if a particular data center—or an entire region—experiences disruption.[89]

Local technology companies may lack resources that compare with the major cloud providers, whose infrastructure is built to the highest cybersecurity standards.[90] Even localization requirements that mandate that financial institutions keep a local copy of data can compromise its security, by increasing the number of access points to the data and therefore the likelihood of a cybersecurity breach.[91] Data localization requirements can also make it more difficult for financial institutions to identify, prevent, and mitigate cyber threats, by limiting their ability to share information from one jurisdiction with regulators in other jurisdiction.[92]

c. Data localization can inhibit financial regulatory oversight

Facilitating regulatory oversight and law enforcement is another commonly invoked justification for data localization requirements. Many financial regulators express concern that once data leaves the borders of their jurisdiction, they will no longer be able to access it. As noted above, data localization does not necessarily solve the problem of law enforcement or regulatory access to data.[93] Moreover, the opposite is just as likely to be true: data localization requirements can make oversight by financial regulators more difficult.

Data localization requirements are likely to provoke, or encourage, reciprocal requirements in other jurisdictions. Thus, even if localization requirements in a regulator's own jurisdiction did facilitate their access to some financial data, similar requirements in another jurisdiction would impede their access to other important data. Where an international transaction involves two jurisdictions that impose data localization requirements, financial regulators in each jurisdiction would only have a view of half the transaction. This would inhibit the exercise of basic financial surveillance functions like anti-money laundering and fraud detection, as well as broader mandates such as financial stability oversight.

d. Benefits of data transfer for financial institutions

In the absence of data localization requirements, financial institutions are able to leverage out-of-jurisdiction cloud technology infrastructure to lower costs, increase data security

[88] Id.
[89] Id.
[90] Id.
[91] Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 JOURNAL OF INTERNATIONAL ECONOMIC LAW 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626 TechRadar Pro, *The high costs of storing data locally in a cloud native era*, TECHRADAR (Feb. 22, 2019), https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.
[92] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (Jul. 2021).
[93] See Section II.c.

and operational resilience, and offer better services to customers. This is true whether the financial institution is a global financial institution looking to enter a new local market, or a local financial institution attempting to gain access to better technology infrastructure or expand globally.

Although many financial services customers still rely on an in-office workforce and in-person services, there is increasing demand for remote work and services, driven in part by the COVID-19 pandemic. Cloud technology facilitates remote work and the provision of digital and other remote services. Financial institutions like Societe Generale, for example, relied on cloud-based device management solutions to support thousands of remote workers through COVID-19-related lockdowns.[94] One Europe-based multinational bank relied on its cloud infrastructure to continue to serve customers in Brazil during the pandemic, which was only possible due to the absence of data localization requirements.[95] Beyond pandemic-driven changes to the workforce and customer service, financial institutions have continued to rely on cloud technology to offer innovative digital services to customers. For example, Itau Unibanco, the largest banking institution in Latin America, leveraged cloud technology to implement Pix, the digital instant payment service mandated by Brazil's central bank.[96] Likewise, BBVA relied on cloud-based technology to securely enable contactless payments while complying with country-specific regulations—making it the first financial institution to offer contactless payments in Peru, Argentina, and Colombia.[97]

Financial institutions can also use offshore cloud infrastructure to deal with financial market disruptions that might otherwise overwhelm their technology infrastructure. Cloud computing allows users to scale up automatically without any physical on-site presence. That can help financial institutions react to market stress events, such as unexpected surges in trading volumes or market volatility.[98] The cloud's automatic scalability, as well as greater processing power compared to traditional technology infrastructure, also enables financial institutions to ingest and analyze data in real-time. For example, cloud solutions make it possible for financial institutions to calculate their liquidity position several times a day, even in during periods of significant market volatility.[99]

In addition, cloud technology facilitates access to frontier technologies like big data analysis and AI, which rely on the vast computing resources available in the cloud. Financial institutions throughout the world already use cloud-based AI tools for basic functions like

[94] MICROSOFT INTUNE, *Société Générale leads the way to the cloud, optimizing user experience and secure device management* (Oct. 14, 2022), https://customers.microsoft.com/en-us/story/1558831416191995829-societegenerale-banking-and-capital-markets-cloud.
[95] INSTITUTE OF INTERNATIONAL FINANCE, *Cloud Computing: A Vital Enabler in Times of Disruption* (Jun. 2020).
[96] BNAMERICAS, *Brazil's Itaú to migrate most of its systems to AWS cloud* (Aug. 4, 2022), https://www.bnamericas.com/en/news/brazils-itau-to-migrate-most-of-its-systems-to-aws-cloud; AMAZON WEB SERVICES, *Itaú Unibanco Accelerates Pix Instant Payment System Development Using AWS* (2022), https://aws.amazon.com/solutions/case-studies/itau-pix/.
[97] AMAZON WEB SERVICES, *BBVA Uses AWS CloudHSM to Enable Fully Compliant NFC Payments* (2021), https://aws.amazon.com/solutions/case-studies/bbva/?did=cr_card&trk=cr_card.
[98] RISK.NET, *Technology innovation of the year* (Feb., 2021), https://www.scotiabank.com/content/dam/scotiabank/corporate/news/assets/Technology_innovation_of_the_year_Scotiabank_Risknet.pdf.
[99] Id.

customer support.[100] As machine learning and AI capabilities develop, it will be used for data analysis and other, more critical functions such as risk management. HSBC, for example, uses cloud-based risk modelling tools to manage risk and inform trading and credit activity.[101] Itau Unibanco moved its machine learning infrastructure from on-premises data centers to the cloud in order to accelerate model deployment and analysis.[102] These sophisticated capabilities, however, will only be available to financial institutions that are permitted to access cloud-based services that, in many cases, will rely on out-of-jurisdiction technology infrastructure and require international data transfer.

PART IV: POLICY RECOMMENDATIONS FOR FINANCIAL REGULATORS

Data localization requirements impose significant costs on financial institutions and the customers they serve. Although they are often motivated by legitimate policy aims, such as protecting sensitive data and ensuring data access for regulatory supervision and enforcement, those aims would be better served through policies that avoid those costs. Financial regulators must strike a balance between the policy concerns underlying data localization requirements and the imperative of facilitating cross-border data flow in the financial sector, including the use of out-of-jurisdiction cloud infrastructure. That balance would be better achieved by rules that: (1) focus on realizing policy objectives directly, rather than indirectly through data localization requirements; and (2) address policy aims through coordination and cooperation with other local regulators and regulators in other jurisdictions.

a. Adopt a principles-based approach to data protection

Mandating that data remains in a particular jurisdiction is neither necessary nor sufficient to maintain its security. Sensitive data that is not managed securely can be compromised by someone who lacks physical access to it. Accordingly, data localization does little to ensure that private data remains private. In order to protect private data, financial regulators should focus on ensuring that data is stored *securely*—whether it is stored locally or abroad. As noted above, the platforms of the major cloud providers are built to give financial institutions tools to implement stringent security requirements, including built-in data encryption.

To alleviate concerns that financial institutions may transfer sensitive data to jurisdictions that do not protect data privacy, regulators might require that data is only stored in a jurisdiction that affords sufficient legal protections to personal data. The approach of the

[100] MICROSOFT, *PicPay integrates Microsoft Artificial Intelligence into service channels* (Jun. 20, 2023), https://news.microsoft.com/es-xl/picpay-integrates-microsoft-artificial-intelligence-into-service-channels/; TRANSBANK, *Transbank further consolidates its position as a tech company with generative AI* (Feb. 19, 2024), https://ir.transbank.cl/en/transbank-further-consolidates-its-position-as-a-tech-company-with-generative-ai; AMAZON WEB SERVICES, *How NatWest Bank Personalizes the Customer Experience Using AWS* (2023), https://aws.amazon.com/solutions/case-studies/natwest/?did=cr_card&trk=cr_card.

[101] GOOGLE CLOUD, *HSBC: Embracing the cloud to lower risk exposure through rapid insight and analysis capabilities*, https://cloud.google.com/customers/hsbc-risk-advisory-tool.

[102] AMAZON WEB SERVICES, *Itaú Improves Speed to Market and Productivity of ML Solutions Using Amazon Web Services* (2024), https://aws.amazon.com/solutions/case-studies/itau-ml-case-study/?did=cr_card&trk=cr_card.

OECD Privacy Guidelines to personal data transfer is instructive.[103] Those guidelines, which were adopted in 1980 and revised in 2013, emphasize that legal responsibility for personal data applies without regard to the location of the data—whether it is stored locally or abroad. They also stipulate that countries should refrain from restricting the cross-border flow of data where sufficient safeguards exist to ensure that personal data is protected. In addition, they provide that restricts on the cross-border flow of personal data should be proportionate to the risks presented.[104]

Brazil's data protection regulation adopts a similar approach. The regulation allows the transfer of data to countries with an "adequate level of protection" for personal data and guarantees of compliance with the data protection rights and principles provided by Brazil's data protection regulation.[105] Importantly, those standards are not rigid, but can be satisfied in several different ways, including through specific contractual provisions or general codes of conduct.[106] That allows financial institutions flexibility to determine how best to protect sensitive data that is transferred out-of-jurisdiction, as long as sufficient privacy safeguards are in place.

b. Focus on the quality of technology infrastructure, not its location

Data localization is often justified based on the notion that local data storage means that the data is more readily available and more resilient to disruption. But the location of data is just one factor that might affect availability and operational resilience. An approach that prioritized availability operational resilience should take into account the many factors that might affect the integrity and availability of data. In many cases, relying on a major cloud provider—including its out-of-jurisdiction infrastructure—will provide financial institutions with a greater degree of availability and resilience than local infrastructure. Regulators should give financial institutions more latitude to make their own assessment regarding the resilience of their data storage and processing solutions to disruption, taking into account the nature and importance of the process and the potential for disruption.

c. Ensure access to data for regulatory supervision and law enforcement

Effective oversight of financial institutions can be achieved without requiring local storage of data. Financial regulators and law enforcement authorities can ensure access to relevant data whether it is stored locally or in a different jurisdiction. Access to data stored abroad can be achieved through agreements with financial regulators in other jurisdictions. Several financial regulators have worked with their foreign counterparts to develop bilateral legal frameworks and mechanisms for cross-border cooperation, which are aimed at enabling cross-border data flows while ensuring access to data for purposes of supervision. The Central Bank of Brazil, for example, has agreements, aimed at facilitating supervisory information flows, with supervisory authorities where Brazilian financial institutions have foreign operations and those where foreign financial institutions have

[103] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
[104] Id, Part IV.
[105] Law on General Data Protection, Section V.
[106] Id.

operations in Brazil.[107] Similarly, the Monetary of Singapore has entered into agreements with U.S. and U.K. financial regulators that allow financial institutions to transfer financial data, including personal information, across border as long as financial regulators have full and timely access to that data.[108] On the multilateral level, the updated Multilateral Memorandum of Understanding developed by the International organization of Securities Commissions (IOSCO) requires signatories to share certain information with regulatory counterparts.[109]

Access to relevant data can also be ensured through financial institutions' contractual arrangements with technology service providers. Several jurisdictions, for example, require that a financial institution's contractual arrangements with its service providers ensure that financial regulators have sufficient data access to supervise the financial institution.[110] These contractual provisions typically include access to the financial institutions' data as well as the cooperation of the service provider with the regulator in relation to information requests and rights of access for audits of the service provider.[111]

d. Increase coordination at the local and international level

The complex patchwork of data localization requirements both within jurisdictions and across different jurisdictions increases costs for financial institutions and stifles competition that would otherwise benefit their customers. To minimize uncertainty and achieve regulatory coherence, financial regulators should work together with local authorities (such as privacy authorities and regulators in other sectors) as well as foreign counterparts to develop broadly consistent approaches to data transfer that would allow for cross-border data transfer while also addressing perceived reasons for data localization. Doing so minimizes unnecessary barriers to data transfer, allowing financial institutions to benefit from out-of-jurisdiction technology infrastructure, including cloud computing.

International coordination can occur at the bilateral level. For example, Australia and Singapore entered into a "digital economy agreement" which allows businesses, including in the financial sector, to transfer data across borders without being required to build or use data centers in either jurisdiction. Importantly, the agreement ensures that privacy rules applicable to personal information continue to apply whether data is stored locally or in

[107] BANCO CENTRAL DO BRASIL, *International MoUs for Supervisory Purposes*, https://www.bcb.gov.br/en/financialstability/supervisionmous.
[108] U.S. DEPARTMENT OF THE TREASURY, *United States – Singapore Joint Statement on Financial Services Data Connectivity* (Feb. 5, 2020), https://home.treasury.gov/news/press-releases/sm899; U.S. COMMODITY FUTURES TRADING COMMISSION AND THE MONETARY AUTHORITY OF SINGAPORE, *Cooperation and the Exchange of Information on Financial Technology Innovation* (Sep. 13, 2018), https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; MONETARY AUTHORITY OF SINGAPORE, *Singapore and UK to Enhance Cooperation in Data Connectivity, Talent Development, Green Finance and Cybersecurity* (Jun. 13, 2019), https://www.mas.gov.sg/news/media-releases/2019/singapore-and-uk-to-enhance-cooperation.
[109] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (May 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.
[110] AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY, *Prudential Standard CPS 231: Outsourcing*, par. 34 (Jul., 2017), https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.
[111] Id.

the other jurisdiction.[112] Singapore has entered into similar agreements with Korea and the United Kingdom.[113]

At the multilateral level, Japan has proposed the concept of "data free flow with trust," which has been endorsed by both the G7 and G20.[114] The aim of the concept, which articulates principles for data governance that would inform global standards, is to promote the free flow of data while protecting the privacy and security of data. In the Indo-Pacific, the Asia Pacific Economic Cooperation (APEC) forum developed a Cross-Border Privacy Rules (CBPR) system, a government-backed privacy framework that establishes a certification mechanism for private companies that agree to implement internationally recognized data privacy protections.[115] Certified companies, whose compliance is assessed by designated accountability agents and is enforcement by law, can freely transfer data between participating countries, allowing them to bridge differences between the privacy laws of participating countries.[116] Several APEC members, including the United States and Japan, have promoted a global CBPR system to expand on the APEC model.[117] Currently, however, financial institutions generally cannot be certified because of financial regulators do not participate in the system.[118]

In the financial sector, the Financial Stability Board (FSB) has identified cross-border data exchange and message standards as a priority for enhancing cross-border payments.[119] As part of this process, the FSB plans to develop recommendations for promoting alignment and interoperability across different data frameworks that apply to cross-border payments, including data privacy, operational resilience, AML/CFT compliance, and regulatory and supervisory access requirement. Those recommendations, in turn, will serve as the basis for national authorities to reevaluate their own data frameworks.[120] Consistency between jurisdictions on the transfer of financial data, and the elimination of barriers to cross-border data transfers, will allow financial institutions to realize the benefits that cloud technology has to offer.

---

[112] Ministry of Trade and Industry Singapore, *Singapore-Australia Digital Economy Agreement (SADEA)* (2020), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.
[113] Ministry of Trade and Industry Singapore, *Korea-Singapore Digital Partnership Agreement (KSDPA)* (2022), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA; Ministry of Trade and Industry Singapore, *UK-Singapore Digital Economy Agreement (UKSDEA)* (2022), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA.
[114] G7, *G7 Roadmap for Cooperation on Data Free Flow with Trust* (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.
[115] Asia-Pacific Economic Cooperation, *APEC Cross Border Privacy Rules (CBPR) System* (2019), https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf.
[116] Id.
[117] U.S. Department of Commerce, *Global Cross-Border Privacy Rules Declaration*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.
[118] Institute of International Finance, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (Mar. 2019).
[119] Financial Stability Board, *G20 Roadmap for Enhancing Cross-border Payments* (Feb. 23, 2023), https://www.fsb.org/wp-content/uploads/P230223.pdf.
[120] Id.

Program on International Financial Systems (PIFS)
134 Mount Auburn Street, Cambridge, MA 02138
www.pifsinternational.org