March 2019
DATA FLOWS ACROSS BORDERS
OVERCOMING DATA LOCALIZATION RESTRICTIONS

Many of the impediments to the flow of data across borders stem from legitimate public policy objectives, such as privacy, security or law enforcement. Yet those restrictions can also bring some side effects for the financial system and the overall economy: they may increase IT and data complexity; undermine the risk management, cyber security and anti-money laundering practices of financial institutions; as well as reducing access to financial services and markets in some countries.

This paper proposes some alternate ways of achieving the desired public policy goals, within a framework of international cooperation that facilitates data flows across borders.

1. DATA LOCALIZATION REQUIREMENTS AROUND THE WORLD

Restrictions to the movement of data across national borders are not new, but they have soared in the last decade, parallel to the development of digital technologies and the associated growth in the storing, processing and sharing of data. On the grounds of law enforcement, national security, personal data protection or economic protectionism, a growing number of jurisdictions have introduced or strengthened different versions of data localization requirements that impede or make costlier the offshore processing of data generated within their territory. This global trend has been particularly pronounced in the Asia-Pacific region, with recent regulatory initiatives in India, Indonesia and Vietnam that have caused concerns for global companies.

Data localization requirements vary across jurisdictions in terms of both their scope of application and their strictness. Whereas some restrictions apply to almost any data that has been collected or generated within the country, other requirements are more targeted and apply only to certain categories of data or to specific economic sectors. Personal data (i.e. information relating to an identified or identifiable citizen), business records, financial data, public data or health information are among the most common targets of data localization restrictions. For sectors, financial services, online service providers, the public sector and telecommunications are the ones that account for the greatest number of non-horizontal requirements.¹ Indeed, in many jurisdictions, financial institutions have faced restrictions to offshore the storing and the processing of data through financial regulation well ahead of the introduction of more general data localization restrictions in the context of data protection and/or cybersecurity laws.

Based on their strictness, data localization requirements can be classified into three categories: i) local-only storing, transmission, and processing; ii) allowing hosting, transmission and processing abroad as long as a local copy is kept current; and iii) narrower, conditional restrictions.

¹The European Center for International Political Economy has compiled a detailed database of data localization restrictions; for more information, see http://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/
1.1. **Local-only storing, transmission and processing**

In the most stringent form of data localization, companies are required to store, transmit and process data exclusively in and between servers or data centers located within the national territory. This can be expressed in the legal framework as either an obligation to locally manage data or as a prohibition of international data transfers. Russia is one of the few countries that imposes this type of hard restriction to a very broad category of data, since the recording, systematization, accumulation, storage, update, amendment and retrieval of personal data of Russian citizens has to be made using databases and networks located in the country. This is being interpreted as an obligation to process data in Russia “in the first place,” although subsequent data transfers are not always precluded.  

Other countries impose hard restrictions only to more specific industries or categories of data, with financial services being a common target of these. For instance, the People’s Bank of China prohibits the analysis, processing and storage of personal financial information outside of the country, although some exceptions have been introduced to allow certain data transfers to offshore headquarters or branches. Similarly, Turkey requires banks and payment systems operators to have their information systems within the national territory, and the Reserve Bank of India (RBI) has mandated since October 2018 that all payment system providers ensure that their entire payments data are stored only in India. Outside of the financial sector, countries such as Australia prohibit personal electronic health information from being held or processed outside of the country.

A hard version of data localization restrictions is currently being discussed in Indonesia, where the Government has proposed a legal amendment that would require “strategic electronic data” to be processed, transmitted and stored in onshore data centers, with a prohibition on delivering, exchanging or copying that data to overseas locations. The current text of the regulation includes a data localization requirement which is less strict — data may be processed offshore but there must be a copy and disaster recovery centers in Indonesia — but broader (and uncertain) in scope.

1.2. **Local copy of data**

Under this type of restriction, companies are required to keep a copy of data in local servers or data centers at all times. This does not always prevent them from transmitting and processing data abroad, but they have to constantly replicate the information — including changes and updates — inside the country. This obligation is usually accompanied by the requirement to have at least some data processing capabilities within the national territory, for backup or disaster recovery purposes. All these obligations increase the relative cost of the offshore.

---

2 For more information on the Russian Data Protection law, see: [https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)


4 These obligations are set in the Regulation on Internal Systems and Internal Capital Adequacy Assessment Process and in the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions. For more information, see: [https://uk.practicallaw.thomsonreuters.com/7-520-1896?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a205157](https://uk.practicallaw.thomsonreuters.com/7-520-1896?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a205157)

5 This includes the full end-to-end transaction details and the information collected, carried or processed as part of the message or payment instruction. For more details, see the RBI’s Notice on the Storage of Payment System Data.

6 Electronic data would be considered strategic when it “affects the public interest, public services, the continuity of the State’s administration or State’s defense and security”. Sectoral agencies and regulators will be able to identify which pieces of information fall within this category. For more details on the Regulation on Electronic Systems and Transactions, see: [https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/general-data-localization-requirements-in-indonesia.pdf?la=en](https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/general-data-localization-requirements-in-indonesia.pdf?la=en)
processing of data and may therefore lead in practice to similar unintended consequences to on-soil storage and processing requirements.

This version of data localization restrictions is currently being proposed in India for the broad category of personal data. The draft Personal Data Protection Bill would require companies to store on a server or data center located in India “at least one serving copy” of personal data that has been collected, disclosed, shared or processed within the country. The Government could exempt certain categories of data from this requirement, but it could also impose a stricter requirement of local-only processing to other categories identified as “critical personal data.” Meanwhile, in Vietnam, the new Cybersecurity Law that entered into force in January 2019 requires online service providers (broadly defined) to store the personal data of national citizens inside the country for at least some period time. In Argentina, an official communication issued by the central bank in November 2007 allowed the outsourcing of IT services to third parties, but required certain datasets to be kept within the country.

In China, the broad data localization restrictions introduced since 2017 by the Cyber Security law and the subsequent regulations and rules cannot be easily categorized. The law requires that personal data and “important data” held by “critical information infrastructure operators” are stored within the country. Although the offshore processing of this data is not explicitly forbidden, international transfers are only allowed if there is a “genuine need for reasons of operational necessity” and they are subject to security assessments, prior regulatory approval and informed customer consent. The draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data — that develops certain aspects of the law — has introduced more uncertainty since all “network operators” and not only those of “critical information infrastructure” appear to be subject to the hard data localization restrictions.

1.3. Conditional restrictions

In this third category of restrictions, international transfers of data are only allowed if certain conditions are met by the company carrying out the transfer and/or by the recipient country. Requirements imposed on the companies may include special security safeguards, certain contractual clauses with the involved offshore parties (affiliates or third-party vendors) or obtaining informed consent from customers. Conditions on the recipient countries generally relate to the extent and enforcement of data protection laws and to any other legal provisions that affect the authorities’ access to data for law enforcement, financial supervision or security reasons. Depending on the specific requirements, these conditional frameworks can de facto prevent the transfer of data to certain locations or reduce the economic case for the offshore processing of data in general.

The European General Data Protection Regulation (GDPR) follows a conditional approach to the transfer of personal data outside of the European Union. On the one hand, transfers are allowed under no additional requirements to those countries that the European Commission recognizes as ensuring “an adequate level of protection”, based on their legal framework, independent supervisory authorities and international commitments. Transfers of personal data to any other country require that companies provide appropriate

---

7 For more information, see the full text of the draft Personal Data Protection Bill.
8 Identifiable personal data and other information such as job titles or medical records must be stored always in Vietnam, whereas data created by the users and information on their social connections will have to do so for at least 3 years. For more information, see: https://www.hldataprotection.com/2018/11/articles/international-eu-privacy/update-vietnams-new-cybersecurity-law/
9 The concept of “important data” is broadly defined in the draft Measures as information “in relation with national security, economic development, as well data closely related to the interest of the society as defined by relevant national standards and guidelines”. For more information on the Chinese Cyber Security Law and its developments, see: https://www.lexology.com/library/detail.aspx?g=dbe04c03-7990-4e0d-8368-e0170637de08
safeguards, generally by adopting binding corporate rules (for transfers within multinational companies) or by introducing standard data protection clauses — adopted or approved by the Commission — in the contracts with third-party service providers.10

The European Union approach to international data transfers is gaining adoption outside of the EU. Argentina already follows a similar approach to international data transfers, and the new Data Protection Bill that the Government submitted to Congress in October 2018 would bring the country even more aligned with Europe’s GDPR.11 That is also the case in Brazil, where the new General Data Protection Law was adopted in August 2018 and will enter into force in February 2020. International data transfers will only be permitted in certain situations, including when recipient countries ensure an adequate level of data protection, when approved legal mechanisms (such as model contract clauses) are employed or when data subjects have provided their consent.12

2. GOVERNMENTS’ OBJECTIVES AND SIDE EFFECTS FOR THE FINANCIAL SYSTEM

Generally, countries introduce data localization restrictions for a combination of public policy objectives, though only some of them are usually openly put forward by Governments. The protection of their citizens’ personal data, the safeguarding of national security, and the access to data for regulatory supervision or law enforcement purposes are generally the most claimed reasons. However, other more underlying goals may include economic protectionism, national sovereignty or even Government control (and surveillance) over the Internet.

Below we discuss some of these intended goals as well as the negative side effects that data localization restrictions may have on a country’s access to financial services and markets as well as for cyber security, risk management, fraud or financial crime.

2.1. Personal data protection

The explosion in the collection and processing of personal data has raised concerns over the risks for consumers if their information is not adequately used by companies and safeguarded against potential security breaches. As a result, countries around the world are developing more comprehensive data protection regulations that set the legal basis for processing personal data, grant citizens certain rights over their own information (e.g. access, rectification or erasure) and introduce security and transparency obligations for data controllers and processors. In this context, it is not only legitimate but reasonable that governments aim to make sure that these protections are not weakened when their citizens’ data is moved to foreign locations with different regulatory regimes and levels of protection. Therefore, some form of conditional restrictions to the international transfer of data may be necessary and are generally recognized and supported by financial institutions, who have a common interest to protect their clients’ personal information. However, stricter, unconditional restrictions are hardly justifiable on the grounds of personal data protection.

2.2. National security

On the one hand, access to sensitive information by foreign governments (or para-governmental institutions) can be a threat to national security. The sensitivity of a particular category or set of data is not only something

10 For more information on the EU regulatory framework for international data transfers, see: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en
11 For more information on the new Bill, see: https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/
12 For more information on Brazil’s new Data Protection Law, see: http://www.mondaq.com/brazil/x/737694/data+protection/Brazils+New+Data+Protection+Law+The+LGPD
relative, but increasingly difficult to assess given how new technologies such as Artificial Intelligence and Machine Learning can generate unforeseen insights from the combination of different sources of data.

In some countries, government agencies might gain relatively easy access to any information stored within their territory, even if there is no clear law enforcement justification. Therefore, it is reasonable that other governments aim to prevent the transfer of data to those countries that do not offer sufficient guarantees. However, as in the case of personal data protection, this can be achieved by making use of conditional and proportionate restrictions.

On the other hand, but closely linked to the former, Governments regard some data processing centers and organizations, including financial institutions, as critical infrastructures for their national security and sovereignty. Certainly, the interruption of some data processing and networking activities — such as those linked to the provision of communication or financial services — can severely damage the functioning of a country, which justifies special resilience, recovery and continuity requirements for those infrastructures. However, it is questionable that requiring that those are located exclusively within the national territory makes them safer, particularly in the case of financial services, which are connected to the global economy.

Faced with localization restrictions, companies may end up using local data processing services that are not best-in-class in cybersecurity — which is always a function of technical, financial, physical, and personnel resources — instead of global cloud-based solutions that may improve resilience and redundancy by relying on a distributed network of computing power. This means that, in cases where a natural or hostile government or hacktivist-engineered disaster disrupts the functioning and reliability of a local data center, workloads can be rebalanced to run on alternate data centers (e.g. in the case of natural disaster, located far away from it), and addressed quickly by provisioning readily-available resources.

In addition, data localization restrictions hinder the sharing of information about cyber-incidents within a company and between industry peers and regulators. Timely access to relevant information is key to effectively responding to cyber-attacks, limiting their impact, as well as preventing future threats.

**2.3. Regulatory supervision and law enforcement**

Supervising compliance with national laws and regulations, and enforcing them when necessary, requires that public authorities (e.g. financial supervisors, tax agencies, Anti-Money Laundering bodies or criminal prosecutors) can obtain access to relevant data on citizens and corporations, under appropriate restrictions and safeguards that balance the rights of the data subjects. When that relevant information is located offshore, national public authorities fear that their capacity to access data may be weakened due to the territorial limit of their powers and potential discrepancies with the laws and authorities of the host countries. Legal access to data may ultimately depend on bilateral or multi-lateral international agreements that can restrict, delay or make costlier the access to information. Therefore, some countries see the requirement of a “local copy of data” as a way of ensuring that they keep full control over access to data for regulatory supervision or law enforcement.

This argument has been particularly relevant for a highly regulated industry such as financial services, subject to a number of different regulations (prudential, market integrity or AML/CFT) that are enforced through active ongoing supervision. As an example, the Reserve Bank of India (RBI) justified its recent data localization requirement for payment service providers on the grounds of “ensuring better monitoring of the growing and highly technology dependent payment ecosystem in the country.” In some jurisdictions, concerns are especially related to the monitoring of market activity by securities regulators, for instance if a small hedge fund stores data on a public cloud located outside of the country and the regulator needs information for an investigation into rogue trading practices.
It is important to understand that modern methods of virtualized data storage mean that data is no longer physically stored such that an authority could seize it without assistance from the data controller. The cooperation of financial institutions and/or their vendors is always necessary for authorities to gain access to information, no matter where a data center is located. This means data localization is irrelevant from a technical perspective and only matters when, absent voluntary cooperation by an institution, authorities need to legally force it. For this, increased and improved cross-border cooperation and mutual assistance between authorities is necessary.

Introducing data localization restrictions instead is counterproductive precisely for some of the ultimate goals of regulatory supervision and law enforcement. By limiting the internal sharing of information across jurisdictions, data localization requirements may undermine the ability of financial institutions to have a “golden source of data” and comprehensive risk management systems (e.g. if exposure to international clients cannot be aggregated across borders). Similarly, data silos may result in suspicious activities not being identified in a timely manner, or missed altogether, undermining the prevention of and reaction to cyber-attacks, fraud, money laundering or terrorist financing.

It is also worth considering whether the supervision of those global institutions may also be affected if the competent authorities in the different jurisdictions where the firms operate cannot share timely and detailed information between them.

2.4. Economic protectionism

Finally, but not least important, some countries introduce strict data localization restrictions with the aim of developing or boosting their national Information Technology sectors. The political argument is quite simple: if companies are required to locally store and process data, they (and/or their service providers) will have to invest in servers and data centers located within the country, which will generate economic activity, employment opportunities and other spillovers associated with high-tech sectors. However, as it is always the case with international trade barriers, the economic consequences are complex and not at all straightforward.

Companies may be forced to use local data processing solutions that are less efficient than those available abroad, such as public cloud solutions that leverage greater economies of scale and provide more flexibility.\(^{13}\) The increased data processing costs will likely be passed on to other companies and in the end, to consumers in the form of higher prices, or even reduced access to services if some data-intensive ones are no longer viable. As argued by the OECD, restrictive data localization requirements “affect firms’ ability to adopt the most efficient technologies, influence investment and employment decisions, increase the cost of innovation and lead to missed business opportunities.”\(^{14}\)

The impact may be particularly negative for the attractiveness of a country for multinational corporations, including financial institutions. Data localization restrictions reduce their ability to benefit from scale-related efficiency gains, make more complex the already difficult task of managing IT infrastructures and data repositories across a global organization, complicate the servicing of clients with presence in multiple geographies, such as in corporate and investment banking, and limit the possibility of combining different sources of data to extract value with artificial intelligence techniques.\(^{15}\) As a consequence, financial institutions

\(^{13}\) For more details, see the IIF paper “Cloud Computing in the Financial Sector: an essential enabler”: https://www.iif.com/portals/0/Files/private/32370132_cloud_computing_in_the_financial_sector_20180803_0.pdf

\(^{14}\) For more information, see: https://www.oecd.org/tad/policynotes/economic-impact-local-content-requirements.pdf

\(^{15}\) Having access to a complete and diverse dataset is essential to reduce the risk of bias in AI developments. Excluding data (completely or partially) from some jurisdictions could skew the behavior of AI based applications in unpredictable ways when deployed to these geographies.
might take a step back in countries that introduce burdensome data localization restrictions, and local economies may lose or have reduced access to global financial services and markets.

It is true that data localization restrictions may reduce competition for local companies, but they will also be less prepared to compete internationally if they cannot access state-of-the-art, more efficient global technologies, as well as financial services and other intermediary inputs. To quantify the potential economic damage of data localization restrictions, the European Centre for International Political Economy (ECIPE) estimated in 2014 the impact on GDP of the proposals that were being discussed at that time in a number of countries. The results ranged from a -0.1% in India to a -1.7% in Vietnam, with general decreases in investment and exports. The paper explains these figures by arguing that “data localization potentially affects any business that uses the internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes.”

3. HOW TO FACILITATE DATA FLOWS ACROSS BORDERS

Some of the aforementioned public policy goals are not only reasonable but desirable: protecting personal data against breaches or inappropriate uses, preserving national security interests or ensuring access to data for regulatory supervision and law enforcement purposes. However, these objectives can be achieved through proportionate and conditional requirements that minimize the downside effects of data localization restrictions, such as increased exposure to cyber threats and reduced ability to manage risks, including preventing and responding to fraud and financial crime. Ultimately, these downside effects have the potential to impact the stability and the integrity of the financial system.

To minimize the cross-border restrictions to the flow of data, international cooperation is essential, particularly to address the challenges related to privacy, security, regulatory supervision, and law enforcement.

International cooperation is currently taking place, and should be reinforced, on three different fronts: trade agreements, which increasingly incorporate free flow of data provisions; cooperation agreements for regulatory supervision or law enforcement; and data protection and privacy, with the mutual recognition of national standards or the development of specific cross-border frameworks. Since free-flow-of-data provisions in trade agreements are always limited by the prevalence of other public policy goals, such as the privacy of individuals or the access to information for law enforcement, those three fronts of international cooperation are necessarily complementary.

**Trade agreements**

Since data localization restrictions are an important non-tariff barrier to trade in the digital economy, they are increasingly being addressed in international trade agreement negotiations. The US has been particularly vocal in trying to include clauses that restrict or minimize the introduction of data localization measures by trade partners. The recent United States, Mexico and Canada Agreement (USMCA) is a good example of this. The Digital Trade chapter prevents the restriction of cross-border transfers of information — with exceptions allowed when necessary for legitimate public policy objectives — and against requiring the use of local computing facilities as a condition for conducting business in the country. 

---

16 For more information, see: [http://ecipe.org/publications/dataloc/](http://ecipe.org/publications/dataloc/)

The Financial Services chapter includes two similar provisions, but makes the latter (on the location of computing facilities) conditional on financial regulatory authorities having “immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party’s territory.”\(^8\) In case an institution fails to provide such access, authorities shall provide “a reasonable opportunity to remediate” before imposing a data localization restriction on that institution. This might in principle be a good solution to minimize restrictions while guaranteeing access to data for regulatory and supervisory purposes, as long as the interpretation of “immediate, direct, complete, and ongoing access” is compatible with the reality of virtualized data storage.

Another recent trade deal, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), currently signed by Australia, Canada, Japan, Mexico, New Zealand, Singapore and Vietnam, includes in its Electronic Commerce chapter both a commitment to allow the cross-border transfer of information for the conduct of business and a prohibition of data localization restrictions.\(^9\) However, non-conforming measures are allowed to achieve legitimate public policy goals, and the financial services industry is excluded. This highlights the importance of improving international cooperation also on the other fronts, to jointly address those legitimate policy goals.

**Cooperation agreements for regulatory supervision and law enforcement**

Authorities require a legal guarantee of their right of access to data even when it is not stored within their jurisdiction. To achieve this, financial regulators from different jurisdictions should develop cooperation agreements between them. As an example, the Monetary Authority of Singapore (MAS) has entered into Memorandums of Understanding (MoUs) with a number of foreign authorities, including the United States Commodity Futures Trading Commission (CFTC) and the Australian Securities and Investments Commission (ASIC). One of the objectives of such an agreement is ensuring that both regulators “have appropriate access to relevant data in their respective licensed trade repositories, whether such trade repositories are located in Singapore or Australia.”\(^\text{20}\)

On the multilateral level, IOSCO created in 2002 a Multilateral Memorandum of Understanding (MMoU) by which signatory authorities agree to provide certain critical information, to permit use of that information in civil or administrative proceedings, to onward share information with self-regulatory organizations and criminal authorities, and to keep such information confidential. IOSCO has recently created an enhanced version of the MMoU with new powers, including compelling subscriber records from telephone and internet communications providers. Similar multilateral frameworks for the exchange of information could be created in other areas of financial regulation.

Beyond the financial sector in particular, the United States enacted in 2018 a federal law (the CLOUD Act) that allows the US Government to enter into executive agreements with foreign governments to create an expeditious procedure for law enforcement access to data across borders.\(^\text{21}\) However, this may compromise citizens’ privacy rights in a manner that is unacceptable to other jurisdictions such as the EU. This shows the


\(^9\) For more information, see articles 14.11 and 14.13 of the Electronic Commerce chapter: [https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf](https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf)


\(^\text{21}\) These agreements would allow participating countries to bypass the Mutual Legal Assistance regime and be able to directly request from US-based companies the data of foreigners that reside outside of the United States, subject to certain safeguards. Reciprocally, participating countries would facilitate the US Government similar access to data.
challenge that the international fragmentation of data protection rules — rapidly developing around the world — poses for the flow of data across borders.

**Data protection and Privacy**

In accordance with the GDPR framework for the international transfer of personal data, the European Commission recognizes certain countries as ensuring “an adequate level of protection” based on their legal framework, independent supervisory authorities and international commitments. Since those countries benefit from no additional restrictions to the inflow of data, this creates an incentive for third-party countries to follow the European data protection standards and seek mutual recognition. Argentina, Canada, Israel, Japan, New Zealand, Switzerland and Uruguay are some of the twelve countries that have so far been recognized by the European Commission as data adequate. The United States is a special case because the Privacy Shield agreement is a specific voluntary mechanism for participating companies, with no general mutual recognition between the US and the EU.

Meanwhile, the Asia Pacific Economic Cooperation (APEC) forum developed in 2011 a Cross-Border Privacy Rules (CBPR) System to which companies can voluntary adhere in order to transfer data between the participating countries, which include, among others, the US, Mexico, Japan, Canada or Australia. Adherent businesses have to implement certain data privacy policies, which are then assessed by designated accountability agents and shall be enforceable by law. Financial services companies cannot generally adhere to the system due to the lack of participation of their competent national authorities. Once again, multilateral international cooperation is needed on different fronts at the same time.
Key recommendations to move forward

A multilateral approach: The flow of data is now a key element of global trade and should be treated as such in multilateral negotiations. It is thus a positive sign that nearly half of the members of the World Trade Organization (WTO) agreed, in the latest Davos forum, to initiate talks on new e-Commerce rules that, among other goals, would seek to address forced data localization measures. Along the same lines, the upcoming G20 summit in Japan will discuss the proposal of Prime Minister Abe to develop a regime for ‘Data Free Flow with Trust’. The financial services sector should not be excluded from those initiatives, which could be then complemented with other arrangements to address the sector-specific concerns.

Interoperable trust mechanisms: Effectively getting rid of data localization restrictions requires some form of cross-border governance arrangements that provide mutual trust on data protection, security and privacy rights. Minimum global standards could be helpful to contain the increasing regulatory fragmentation in those areas. Notwithstanding, given the differences in cultural and social values, data protection frameworks will hardly be homogeneous, and it is therefore essential to develop ‘interoperability’ mechanisms between them, in the form of mutual recognition agreements or specific conduits for the cross-border flows.

Cooperation of financial regulators: Given the specific restrictions, side effects and challenges for the financial sector, global standard setters such as the Financial Stability Board should do a stocktaking exercise that identifies data localization restrictions affecting financial services around the world and assesses their impact on financial stability. The FSB could then raise proposals to foster greater cooperation on access to data between national authorities, so that data localization restrictions can be minimized.
Pablo Urbiola
Policy Advisor
purbiola@iif.com

Other IIF Specialists

Brad Carr
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

Conan French
Senior Advisor for Innovation and Fintech
cfrench@iif.com

Adrien Delle-Case
Policy Advisor
adellecase@iif.com

Daniel Pujazon
Policy Advisor
dpuazon@iif.com