International Principles to Improve Data Security and Mobility to Support Global Growth

GFMA and its constituent bodies AFME, ASIFMA and SIFMA support an open and resilient global economy in which financial services can boost international trade and investment, and global economic growth while protecting individuals' rights to privacy. With the rise of the digital economy, policymakers around the world have rightly strengthened their policies that protect data and privacy, while continuing to enable cross-border trade that contributes to global economic growth.

In this paper, we set out:

- The context of the digital economy and the importance of data privacy and free flow of data
- Policy objectives for supporting the digital economy whilst respecting privacy
- Principles which we would ask that regulators consider in order to support the achievement of those policy objectives.

Context of the digital economy and the importance of the free flow of data

Cross-border trade of digitally-deliverable services is on the rise: Global e-commerce reached almost $28 trillion in 2016,[1] and retail e-commerce alone is estimated to have doubled between 2014 and 2018.[2] These trends have led observers to conclude that "[v]irtually every type of cross-border transaction now has a digital component."[3] As Ravi Menon, Managing Director of the Monetary Authority of Singapore, has noted "(t)he ability to aggregate, store, process, and transmit data – especially across borders – is critical to the digital age."[4] It is also essential to trade, investment and growth: cross-border data flows have increased global GDP by 10 percent over the last ten years.[5] At

[1] U.S. International Trade Commission, "Despite Huge Growth in Global Digital Trade in Recent Years, Some Countries Seek to Slow Adoption, Reports USITC," September 2017, https://www.usitc.gov/press_room/news_release/2017/er0928ll836.htm.

[2] Retail e-commerce sales worldwide from 2014 to 2021, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

[3] McKinsey, "Digital globalization: The new era of global flows," March 2016, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[4] https://www.bis.org/review/r181112a.pdf

[5] Ibid.

the EU level, for example, it is estimated that tackling data fragmentation could generate an additional growth of up to 4% GDP for the European data economy by 2020 which could be worth more than EUR 106 billion in 2020,[6] and benefit the EU GDP by €8 billion/year alone.[7] Digital trade is important for every sector of the economy and supports the local manufacture of goods, production and trade of agriculture, and research and development of new innovations. Financial services stimulate a multiplier effect for trade and investment by manufacturers in economies worldwide. In this new digital economy, privacy, data security and efficiency are critically important to businesses, governments, and consumers.

Despite the positive impact of digitization on global growth, several jurisdictions have taken steps to limit the cross-border transfer of data by introducing new data localization requirements that inhibit the further rise of digital trade. By data localization we refer to national or regional laws and regulations that require firms to store, process, or handle data within geographic borders. Some jurisdictions have introduced related measures that require the use of certain technology goods or services that are produced locally. Data flows are also impacted by employment laws and outsourcing restrictions. Data localization policies have quadrupled since 2000 (see appendix I).[8] The most common data localization measures target banking, company records and accounting data.[9] Limitations on the free flow of data have serious implications for global firms, the end-users they serve, and economic growth more generally.

Policymakers prescribe data localization requirements with the intention to improve resilience of key financial services, protect privacy and increase data security. In furtherance of these objectives, they sometimes consider that requiring local servers or computing facilities will foster innovation, spur technology transfer, or bolster domestic economic growth. In reality, resilience, privacy, and security is best addressed through the enforcement of rigorous and high-standard systems, which the financial institutions that we represent share the desire to maintain in their efforts to optimize operational resilience. A global technology network architecture best supports effective delivery of goods and services, protection of data in transit and at rest, and ability to reduce costs while complying with regulations. Financial institutions of global reach are able to offer services to customers wherever they travel or do business, they can protect clients with global cyber risk management operations, and

[6] European Data Market study, SMART 2013/0063, IDC, 2016, February 2013, https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report_030417_2.pdf
[7] European Commission, "State of the Union 2017: Free Flow of Non-personal Data", September 2017, http://europa.eu/rapid/press-release_IP-17-3190_en.htm
[8] U.S. International Trade Commission, "Despite Huge Growth in Global Digital Trade in Recent Years, Some Countries Seek to Slow Adoption, Reports USITC," September 2017, https://www.usitc.gov/press_room/news_release/2017/er0928ll836.htm, page 414.
[9] European Centre for International Political Economy (ECIPE), "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016, http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

promptly respond to requests for data from regulators and law enforcement officials while reducing costs to customers and shareholders.

Furthermore, data localization requirements and policies that hinder the free flow of data increase cyber risks and erect barriers to trade, competition, and innovation. Data localization not only impairs financial services firms' ability to serve their customers and the economy, but also negatively impacts overall data protection and creates inefficiencies. For example, from a security standpoint, data localization multiplies entry-points for bad actors to target while negatively impacting threat visibility and responsiveness. In terms of its economic impact, the resources required for compliance with data localization laws often deter firms from entering or expanding in a market, limiting competition, innovation job creation and investment. The increased costs for those firms who do enter the relevant market passed along to consumers, reducing their access to goods and services. The costs of data localization policies ultimately constrain the rise of digital trade, as well as global economic growth. The Information Technology and Innovation Foundation, analyzing multiple economies, estimates that barriers to cross-border data flows decrease GDP by between 0.1 to 1.7 percent.[10] The European Centre for International Political Economy (ECIPE) argues that introducing comprehensive data localization measures in each EU Member State would lead to "a loss of EU-wide output by 52 billion euros per year" which amounts to 0.37% of GDP.[11]

The financial services industry supports global regulatory authorities' legitimate concerns to protect the privacy of consumers and investors and the integrity of financial data. We also recognize that financial institutions must provide appropriate data to regulators for them to perform their regulatory and supervisory roles. However, policymakers should reconsider translating those objectives into measures that create barriers and do not accomplish those objectives. These measures are ineffective and have many negative implications for the digital economy and economic growth. As a consequence, regulators should develop alternative tools, based notably on regulatory and supervisory cooperation, to data localization policies in order to ensure privacy protection and data integrity.

The location of computing facilities or the use of Cloud services have no bearing on the ability of financial institutions to ensure access to data for regulatory or supervisory purposes. The uptake of Cloud services is increasingly important for supporting the development of more efficient financial products and markets and in providing innovative and secure data and services to consumers, as expressed by representatives of the European Commission at the round table on 'Financial Services in the Digital Era' in May 2017, which singled out Cloud computing as a "pivotal technology for EU

[10] ITIF, "Cross-Border Data Flows; Where Are the Barriers, and What Do They Cost?" May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
[11] European Centre for International Political Economy (ECIPE), "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016, http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

competitiveness."[12] However, for this to be realized all industry participants will need to address the risk of regulatory fragmentation across jurisdictions as Cloud service uptake increases and associated policy is developed. At the regional and global level the regulatory landscape needs to continue to embrace the principles of free flow of data, resilience, privacy, and security and the realities of Cloud technology. This can be achieved by adopting a proportionate approach to Cloud outsourcing that encourages its uptake while addressing any potential supervisory concerns. Both policymakers and financial institutions will need to collaborate, to ensure that there is sufficient information provided to regulators to enable them to perform their financial stability and market oversight objectives where Cloud services are used, without creating vulnerabilities in firms' financial crime programs or engaging in digital protectionism. Regulation should recognize modern methods of data storage and processing and manage its risks, not prevent it, in order to realize the benefits of modern data storage related to outsourcing, cyber security and cloud services.

Impact on Financial Services

The financial services industry has evolved within the digital economy to leverage advances in information technology to enhance the quality, efficiency, and resiliency of financial services provided to investors and end-users across the globe. Accordingly, we encourage policymakers to support the financial services sector, and the end-users it serves

Transferring data across borders is crucial for the financial services industry to: (i) provide core products and services to customers, including executing buy and sell orders in global markets, all the more as regulations often have extraterritorial reach and require more data to be incorporated into orders; (ii) manage risk on a holistic basis across affiliates and borders; and (iii) comply with financial regulatory requirements in various jurisdictions, including Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations; and (iv) monitor and defend global networks from malicious cyberattacks. In addition, cross-border data flows are necessary to support the development of financial technologies (fintech), including blockchain applications.

The financial services sector has been adversely impacted by restrictions on cross-border mobility of data in several jurisdictions globally, such as: (i) blocking statutes without appropriately targeted exceptions; (ii) unnecessarily restrictive privacy requirements; (iii) requirements to store data onshore by establishing inefficient in-country servers and data centers; and (iv) outsourcing restrictions. Recognizing governments responsibility to protect privacy of consumers and data integrity, these types of measures are counterproductive at the global level, as they fragment the global operations of firms, inhibit the defense of networks and data, impose inefficiencies and costs, thereby inhibiting cross-border trade and investment. Details are given below.

[12] https://www.bbva.com/en/financial-services-era-cloud-computing/

On November 14, 2018, the European Parliament and the Council of the EU approved a legislative reform banning data localization restrictions in the EU. The new Regulation (EU) 2018/1807 ("Regulation"), was published in the Official Journal of the EU on November 28, 2018 and will be applicable in all EU member states as of 28 May 2019.[13] The Regulation creates a framework for the free flow of electronic non-personal data in the EU, which is limited today in many EU member states by localization restrictions or legal uncertainty in the market. It foresees the elimination of any data localization requirements at national level, except for reasons of public security. The Regulation also facilitates regulators' access to data, the adoption of Cloud computing and increased data portability between cloud services providers.

One key challenge of this Regulation is for global firms that operate both directly and indirectly (i.e. via their vendors) in an intra-EU environment. These firms may find storing and processing data in the EU difficult due to the increasing complexity of compliance, such as data protection regulations and employment and outsourcing laws. Equally, firms will need to manage how EU personal data rights are attached to non-EU data by virtue of the data being held and processed in the EU. The European Commission is now tasked with issuing guidance on how this Regulation and GDPR apply to such mixed datasets by 28 May 2019.

The recently signed U.S. Mexico Canada Agreement (USMCA) provides another example of data provisions. It includes a free flow of data provision, which updates the approach from the GATS Understanding reached in 1997. USMCA also included a prohibition on local data storage requirements in circumstances where a financial regulator has the access to data that it needs to fulfill its regulatory and supervisory mandate.

International Principles to Improve Data Privacy, Security and Mobility

The financial services industry supports global regulatory authorities' legitimate concerns to protect the privacy of consumers and investors and the integrity of financial data. We encourage global regulators to consider the following principles and adopt best practices to improve data protection and mobility—which we believe are mutually reinforcing—while continuing to foster data privacy.

1. **Recognize that the ability to transmit data across national boundaries and store data in different jurisdictions, with adequate protections, is fundamental to supporting a secure, innovative, and prosperous global financial system, as well as fostering global economic growth.**[14]

[13] https://eur-lex.europa.eu/eli/reg/2018/1807/oj
[14] GFMA, ISDA and EBF, International Cybersecurity, Data, and Technology Principles, May 2016, http://www.gfma.org/correspondence/item.aspx?id=807.

Policymakers have a significant interest in reducing barriers to safe and efficient data flow to create an enabling environment to grow the digital economy. Regulations and legal requirements on data protection can function as non-tariff barriers to trade and restrict economic activity when they are not aligned with international standards and best practices. By recognizing the impact that privacy and data protection policies have on international trade and investment, policymakers can tailor their approach to meet their objectives to protect individuals' rights to privacy while also bolstering the fight against financial crime and enabling economic growth. Policymakers should support common frameworks that multinational financial institutions can implement in a global operating environment. Cooperative agreements between governments on cross-border enforcement, supervision and data sharing can be put in place to support access to data, while addressing financial market integrity and sovereign risks.

Developing interoperability between the privacy laws and regulations of different jurisdictions, such as APEC has done through the Cross-Border Privacy Rule, enables safe and efficient cross-border data flow to improve international trade, catalyze investment, and bolster the uptake of digital channels for trade. For example, as Brexit approaches it is essential that there is clarity as to the ability of business to continue to transfer personal data between the EU and UK.[15]

2. Engage with industry to align regulatory requirements and encourage adoption of international best practice in data security and mobility.

We encourage governments to consult financial services institutions to better understand standards and best practices used to protect data as it is stored and transferred across borders. Eliciting private sector input prior to formulating regulations for privacy and data protection could avoid unintended consequences for trade, investment and economic growth. We also encourage policymakers to reference existing frameworks for managing cybersecurity risk. ISO 27103, the NIST CSF and the Financial Services Sector Profile represent aligned risk management frameworks at the international, national and sector specific levels. We also encourage further adoption of the "International Principles for Cybersecurity, Data and Technology."[16] The path forward in an increasingly digital and technology advanced world includes cooperative agreements between governments to address cross-border resilience, privacy and security, and of markets keen to develop and/or mature their digital-related frameworks and capacity, instead of data localization requirements." Generally speaking, regulators should develop alternative approaches to data localization policies.

3. Recognize that, with adequate control and supervision, cross-border data mobility supports data protection and system resilience.

Well-intentioned, overly restrictive data localization rules may in fact undermine the resilience of the global financial system and individual institutions. Privacy cannot be protected without effective

[15] https://www.afme.eu/en/reports/publications/effective-flow-of-personal-data-post-brexit/
[16] GFMA, EBF and ISDA, "International Cybersecurity, Data and Technology Principles," May 2016, http://www.gfma.org/correspondence/item.aspx?id=807.

security, which depends on *how* data is shared and stored, not *where*. Processing and sharing appropriate consumer data across borders is critical to preventing abuse, particularly in the context of

cybersecurity and sanctions/anti-money laundering enforcement. Undue limitations on cross-border data access inhibit firms' ability to effectively set and enforce technology controls, monitor threats to company networks and infrastructure, and share information with partners and law enforcement agencies to mitigate broader systemic risks. In addition, requirements to store data in fragmented or disparate facilities can create additional points of entry for bad actors to infiltrate networks. Outsourced or consolidate regional data centers or information technology (IT) hubs enable firms to dedicate resources to data and technology security, and ensure there are robust resilience capabilities, such as for data back-ups. In that way, data localization adversely affects firms' business continuity and disaster recovery plans.

4. Enable targeted cross-border information sharing.

Financial institutions must provide appropriate, timely data to regulators to fulfil their regulatory obligations in different jurisdictions. Restrictions on cross-border data flow can introduce compliance risk for firms, as privacy laws and blocking statutes introduce conflicts of law for multinational firms subject to multiple regulatory reporting regimes. Accordingly, data localization policies can prevent financial regulators from having the data necessary to do their jobs effectively, as well as undermine firms' efforts to comply with regulatory requirements. For instance, financial institutions need to share information with their affiliates across borders to obtain information necessary to file suspicious activity reports (SARs) under relevant AML regulations applicable worldwide. We call on policymakers to be mindful of the impact that data localization policies have on firms' abilities to continue to carry out important investor protection protocols, including AML, KYC, or financial crime investigations. We encourage data protection authorities to coordinate with other financial crime and cyber authorities when defining parameters for the use of data to allow targeted cross-border data transfer necessary to fulfil regulatory obligations and enhance investor protection.

5. Enable adequately secure outsourcing arrangements that improve the efficiency and competitiveness of financial services providers.

Outsourcing arrangements are critical to improving the efficiency of the financial services industry, enabling firms to provide superior customer service, maintain competitiveness internationally, and reduce operational costs to boost investments in other areas that deepen local capital markets. Multinational financial institutions often outsource operationally-intensive functions to other affiliates within their group to leverage in-house capabilities in a competitive, efficient, and effective manner. Doing so improves efficiency by enabling financial institutions to maximize use of existing

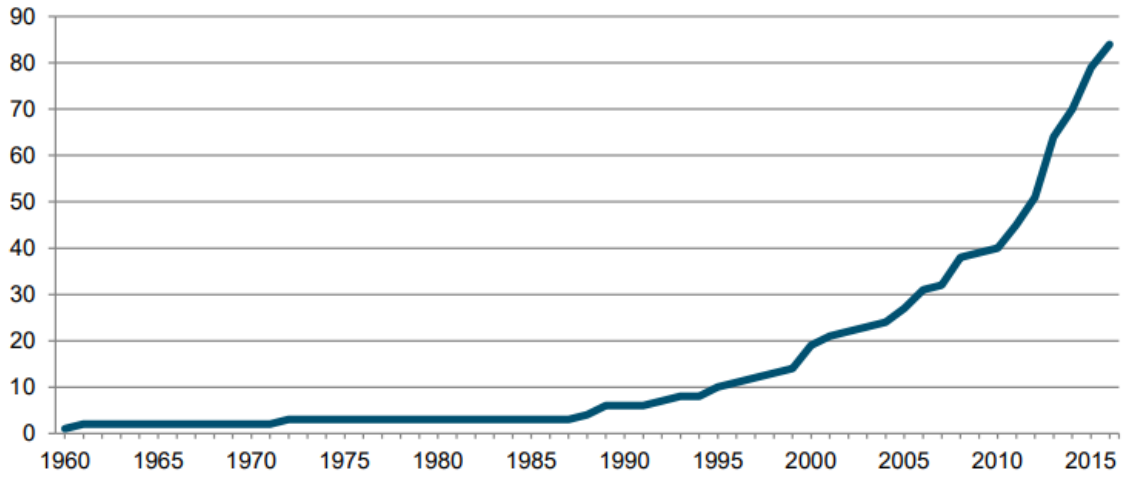
infrastructure, and in turn, increase investments in more productive ways. However, policies that restrict outsourcing arrangements in the financial services sector often result in the de facto localization of data onshore, which deters firms from entering or expanding in a market, undermining economic growth and disadvantaging local consumers. Subject to other overarching regulatory

requirements, policies governing outsourcing should be principles-based, technology and entity neutral, and impartial to geographic location, to allow financial institutions to utilize outsourcing arrangements according to their own business models and risks whereas the relevant authorities should not look to introduce new requirements or restrictions beyond existing outsourcing regulations.[17]

[17] AFME response to the EBA Consultation Paper on Draft Recommendations on Cloud Outsourcing, August 2017, https://www.afme.eu/globalassets/downloads/consultation-responses/AFME-TAO-Response-to-EBA-Consultation-Paper-on-Draft-Recommendations-on-Cloud-Outsourcing.pdf

Appendix I: Increased Data Localization Measures Globally

Figure ES.1: Number of data localization measures globally (1960–2015)



Source: US International Trade Commission, "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions," September 2017, https://www.usitc.gov/publications/332/pub4716.pdf, *page 17.*