GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

July 2024

SUPPLEMENTAL RECOMMENDATIONS TO THE OECD ON DATA FREE FLOW WITH TRUST

CROSS-BORDER PAYMENTS & FINANCIAL DATA

The Global Data Alliance (GDA)[1] submits the following supplemental recommendations[2] to the Secretariat of the Organisation for Economic Cooperation and Development (OECD) in connection with the Data Free Flow with Trust (DFFT) Expert Community's work on cross-border payments and financial data transfers.

Specifically, we urge the OECD DFFT Community to take into account financial data transfers broadly; regulatory contexts beyond anti-money laundering and personal data protection; and the importance of cross-border access to financial digital tools and data analytics. We further urge the OECD DFFT Community to consider articulating a broader set of principles regarding financial data more broadly, including insurance, banking, securities, accounting, and market research data that reflect the Community's support for cross-border financial data transfers to support various cross-border financial regulatory objectives and other legitimate policy priorities.

Background

The ability to transfer financial data and access financial analytics and other technologies securely across digital networks is critical to many financial regulatory and other policy objectives, including those relating to anti-money laundering, anti-corruption, fraud prevention, financial reporting and transparency, securities regulation, and financial inclusion (hereinafter "legitimate financial regulatory objectives").[3] As stated in the OECD's June 2024 report that analyzed 10 years of data relating to Services Trade Restrictiveness:

> A key business and policy challenge in digital trade today is the rising volume of data localisation requirements affecting business operations, production, and consumption. By early 2023, close to 100 data localisation measures were in force across 40 countries, with more than half of these emerging in the past decade. … More sensitive data, including health, financial and public sector data, are associated with more restrictive data localisation measures. ...
>
> Lowering barriers on financial and professional services is key to enabling other economic activities. With the growing complexity of international business models, market bridging and support services are essential for firms supplying services across multiple markets. For example, financial services ensure access to credit, payment systems, and insurance to scale up production and sales. Trustworthy, transparent, and easy to understand accounting information is needed to assess creditworthiness and to ensure compliance with financial regulations. Legal services are necessary to support operations at home and affiliates abroad, to ensure compliance with regulations, and to

> support the enforcement of contracts. Banking and insurance services support production and exchange in virtually all economic activities.
>
> Market bridging and support services such as financial and professional services have been the most affected by trade impediments over the past ten years, representing close to 30% of all restrictions in the STRI in 2023.[4]

Unfortunately, policies that undermine the ability to transfer financial data across digital networks continue to increase. These restrictions – which tend to undermine various cross-border financial regulatory objectives – exist in a wide range of economies, including Bangladesh, China, India, Turkey, and the United Arab Emirates (among others). For an illustrative list of these restrictions, please see the Annex I.

Against this background, the DFFT Community workstream on cross-border payments and financial data transfers is of particular importance.

OECD DFFT Community Cross-Border Payments Workstream

Given the importance of cross-border financial data transfers to both cross-border financial regulatory objectives and other policy priorities, the GDA strongly supports the DFFT Community's cross-border payments workstream. As the OECD DFFT Community page notes,

> Cross-border payments are expected to grow from USD 190 trillion in 2023 to USD 290 trillion by 2030. Despite this growing trend, elements of cross-border payments remain expensive and slow, leaving the most vulnerable behind and hindering integration and growth. … A key issue in cross-border payments is the wide range of regulations that govern the data flows underpinning them.

As part of a broader effort to address this challenge, the DFFT Community proposes to: (1) identify "specific synergies and/or misalignments between the different laws and regulations that govern payment-related data flows"; and (2) develop a "report mapping payment-related data flow issues, … to inform … which data transfer tools could be most appropriate for data transfers related to cross-border payments."

GDA Recommendations

The GDA supports the OECD DFFT Community's proposed design for the cross-border payments workstream. We further recommend that the OECD DFFT Community consider issuing a broader set of principles regarding financial data more broadly, including insurance, banking, securities, accounting, and market research data. Such principles should support cross-border financial data transfers and cross-border access to financial data analytics tools to support cross-border financial regulatory objectives and other legitimate policy priorities.

Prohibiting data localization and residency requirements, and thus leveraging the power of cross-border data transfers and data analytics to combat regulatory risks, is an international best practice. This best practice has been recognized by regulators from numerous countries. As stated by Singapore and the United States in a joint announcement on cross-border data transfers in the financial services sector earlier this year:

> Data localization requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information. Data mobility in financial services supports economic growth and

> the development of innovative financial services and benefits risk management and compliance programs, including by making it easier to detect cross-border money laundering and terrorist financing patterns, defend against cyberattacks, and manage and assess risk on a global basis.[5]

We also recommend that the OECD DFFT Community take into account the legal norms reflected in relevant international law, such as the UK-Japan Comprehensive Economic Partnership, the Australia-Singapore Digital Economy Partnership, the US-Mexico-Canada Agreement, and the US-Japan Digital Trade Agreement. Each of these agreements reflects the positions of those economies' financial regulators and economic and trade ministries with respect to the cross-border movement of financial data. For example, Art. 8.63 of the UK-Japan CEPA states as follows:

> 1. A Party shall not restrict a financial service supplier of the other Party from transferring information, including transfers of data into and out of the former Party's territory by electronic or other means, where such transfers are relevant for the conduct of the ordinary business of the financial service supplier.
>
> 2. Subject to paragraph 3, a Party shall not require, as a condition for conducting business in its territory, a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.
>
> 3. A Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure access to information that is appropriate for the purposes of effective financial regulation and supervision, provided that the following conditions are met:
>
> > (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and
> >
> > (b) the Party or its financial regulatory authorities consults the other Party or its financial regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.

Similarly, Article 25.2 of the Australia-Singapore Digital Economy Agreement states as follows:

> Neither Party shall require a covered financial person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, provided that the Party's financial regulatory authorities, for regulatory or supervisory purposes, have immediate, direct, complete and ongoing access to information processed or stored on computing facilities that the covered financial person uses or locates outside the Party's territory.

Please see Annex II for a compilation of these and similar provisions that describe various OECD members' financial regulatory and economic officials' determinations regarding cross-border transfers of financial data and the location of computing facilities.

Conclusion

We thank the OECD Secretariat for its support for the DFFT Expert Community Agenda, and we hope that you will take into account these recommendations to map out a future expansion of discussions to focus on cross-border financial data transfers and access more broadly. Should you have any questions regarding this submission, please feel free to contact the GDA at gdainfo@bsa.org.

---

[1] The Global Data Alliance is a cross-industry coalition of nearly 100 companies from around the world that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies support tens of millions of jobs across the globe. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, *see* https://www.globaldataalliance.org

[2] These comments build on our prior DFF comments. *See e.g.,* Global Data Alliance Recommendations To Japan's Digital Agency on Data Free Flow with Trust (Oct. 10, 2023), at: https://globaldataalliance.org/wp-content/uploads/2023/10/10122023gdafreeflowtrust.pdf; Global Industry Statement on An Institutional Arrangement for Partnership on Data Free Flow with Trust (2023), at: https://globaldataalliance.org/wp-content/uploads/2023/04/04182023g7dfftglindustry.pdf; Global Data Alliance, *GDA Comments on an Institutional Arrangement for Partnership on "Data Free Flow with Trust"* (2023), at: https://globaldataalliance.org/wp-content/uploads/2023/04/04212023gdacmtsg7dfft.pdf; Global Data Alliance, *GDA Comments on Japan's 2023 Cross-Border Data Policy Agenda* (2023), at: https://globaldataalliance.org/wp-content/uploads/2023/02/02012023gdajpmeti.pdf; World Economic Forum, *The Case for An Institutional Mechanism for Data Flows* (2023), at: https://www3.weforum.org/docs/WEF_From_Fragmentation_to_Coordination_2023.pdf

[3] https://globaldataalliance.org/sectors/finance/

[4] https://www.oecd-ilibrary.org/trade/revitalising-services-trade-for-global-growth_3cc371ac-en

[5] *See* United States-Singapore Joint Statement on Financial Services Data Connectivity (Feb. 2020), at: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

Annex – Cross-Border Restrictions and Localization Mandates for Financial Data

Name of Measure	Country	Description or Excerpt of Relevant Cross-Border Data Restrictions or Data Localization Mandates	Link
Bank Companies Act	Bangladesh	Section I2 of the Bank Companies Act, I 99 I has imposed a restriction upon bank companies with regard to removal of documents and records outside Bangladesh without prior permission of Bangladesh Bank (i.e. the central bank of Bangladesh). The requirement for obtaining prior written permission from Bangladesh Bank is upon the transferor, i.e. the bank company. Banks must also maintain confidentiality in banking transactions.	Transfer in Bangladesh - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
Administration Measures for Anti-Money Laundering and Anti-Terrorist Financing of Financial Institutions	China	PBOC's AML rule that prohibits to sharing of data to any third parties (including intra-group transfers) indirectly prevents offshoring. Article 5 Customer identity information and transaction information obtained in the performance of anti-money laundering and anti-terrorist financing duties or obligations in accordance with the law shall be kept confidential and shall not be provided to any third party unless otherwise provided by law.	https://www.gov.cn/zhengce/zhengceku/2021-04/16/content_5600189.htm
PBOC 2018 No.19 Notice on Issuing the Guidance for Risk Management of Money Laundering and Terrorist Financing of Locally Incorporated Financial Institutions (Trial), effective 1 January 2019	China	This rule prohibits sharing of data to any third parties (including intra-group transfers) indirectly prevents offshoring. Article 41 ▪ Financial Institutions should strictly protect information obtained from anti-money laundering work conducted in line with China's AML Laws, National Security Laws and Cybersecurity Laws. Unless permissible by law, the information shall not be provided to any institution or individual. ▪ Financial Institutions should implement cross-border information security measures, strictly controlling the cross-border access, scope and degree of information on customers, accounts and transactions involved when conducting cross-border businesses and dealing with cross-border supervision and suspicious transaction reporting. ▪ In the event an overseas authority requires a Financial Institution to provide information on its customers, accounts, transactions or other information for purposes of combating money laundering and terrorist financing, the Financial Institution should inform the counterparty that the request should be made through a diplomatic channel, judicial assistance channel or financial supervision cooperation channel and that such information cannot be provided without authorization from the China regulators.	
CBIRC 2019 No.1 Measures for the Administration of Anti-Money Laundering and Counter terrorist financing of Banking	China	This rule prohibits sharing of data to any third parties (including intra-group transfers) indirectly prevents offshoring. Article 22 ▪ Banking financial institutions and their staff should keep confidential all customer and transaction information obtained when performing their obligations on AML/CTF according to the law and regulations. Unless permissible by law, the information shall not be provided to any institution or individual. Article 28 ▪ Banking financial institutions should not provide customer and transaction information obtained when performing AML/CTF obligations to any overseas party unless stipulated by laws and administrative regulations.	

Financial Institutions, effective 29 January 2019		▪ Banking financial institutions should report to the banking regulatory authority in a timely manner relevant issues concerning the provision of cross-border information, and take corresponding measures in accordance with the requirements of laws and regulations.	
People's Republic of China 2020 Notice No. 12 – Further Safeguarding AML Data Confidentiality, 12 November 2020	China	This rule prohibits sharing of data to any third parties (including intra-group transfers) indirectly prevents offshoring. <u>Article 5</u> • All obligatory institutions should consolidate data resources of AML-related systems and are encouraged to gradually explore and realize centralized storage of anti-money laundering information. • Improve the business process and closed-loop management mechanism of customer identification, suspicious transaction monitoring and investigation, and financial intelligence clue transfer, and strictly control the authority of all departments and all levels of personnel to use anti-money laundering related systems. • Obligated institutions shall keep confidential of 1) customer data and transaction information obtained in accordance with the law to perform customer due diligence, large-value transactions and suspicious transaction reporting obligations, 2) information of monitoring, analyzing, and reporting suspicious transactions and conducting watch list screening in accordance with the law, 3) and information of cooperating with the People's Bank of China's anti-money laundering investigation and adopting temporary freezing measures, and shall not disclose or provide to any unit or individual unless required by law. • Obligated institutions should make it clear that the AML leading department shall submit suspicious transaction reports to the China Anti-Money Laundering Monitoring and Analysis Center in accordance with the law and avoid other internal departments or institutions from reporting suspicious transaction reports or related information.	
Draft Measures for Data Security Management of Accounting Firms	China	On **November 2, 2023**, the Ministry of Finance opened a public consultation on the draft measures for data security management of accounting firms until December 11, 2023. The issued draft measures propose that auditors undergo or conduct additional cybersecurity checks involving national security, specifically applying to auditors hired by domestic firms or conducting cross-border work. It outlines accounting firms' responsibility for the data security of their organizations, with supervisory bodies designated for oversight. Moreover, it includes obligations related to the hierarchical classification of data, data transfer, encryption, backup, and network security. Lastly, the measures outline enhanced systems for supervision, focusing on the finance, energy, communications, transportation, science, and national defense sectors. Violations of the proposed measures would be subject to penalties by the Data Security Law of the People's Republic of China.	
Law 1266 on Financial Data Processing	Colombia	Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CO
Reserve Bank of India, Amendment to the Master Direction (MD) on Know-Your-Customer,	India	Summary: Requires establishment of Video-based Customer Identification Processes (V-CIP) that limit cross-border data transfers, as follows: "(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses."	Reserve Bank of India, Amendment to the Master Direction (MD) on Know-Your-Customer

RBI/2021-22/35 (May 10, 2021)			
Reserve Bank of India, Directive on Storage of Payment System Data (2018)		Excerpt: All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	Reserve Bank of India, Directive on Storage of Payment System Data (2018)
Securities and Exchange Board of India, Advisory for on Software as a Service, (Nov. 3, 2020)	India	Excerpt: Para 3.: "It is advised to ensure complete protection and seamless control over the critical systems at your organizations by continuous monitoring through direct control and supervision protocol mechanisms while keeping the critical data within the legal boundary of India."	Securities and Exchange Board of India, Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions
Insurance Regulatory & Development Authority of India, Maintenance of Insurance Records Regulations (2015)	India	Excerpt: Art. 3(9): The records including those held in electronic mode, pertaining to all the policies issued and all claims made in India shall be held in data centres located and maintained in India only.	Insurance Regulatory & Development Authority of India, Maintenance of Insurance Records Regulations (2015) Khaitan & Co., Data Localization Laws - India
Securities and Exchange Board of India, Framework for Adoption of Cloud Services by SEBI Regulated Entities	India	The cloud services shall be taken only from the Ministry of Electronics and Information Technology (MeitY) empaneled CSPs. The CSP's data center should hold a valid STQC (or any other equivalent agency appointed by Government of India) audit status. For selection of CSPs offering PaaS and SaaS services in India, RE shall choose only such CSPs which: 1. Utilize the underlying infrastructure of MeitY empaneled CSPs for providing services to the RE. 2. Host the application/ platform/ services provided to RE as well as store/ process data of the RE, only within the data centers as empaneled by MeitY and holding a valid STQC (or any other equivalent agency appointed by Government of India) audit status.	Securities and Exchange Board of India, Framework for Adoption of Cloud Services by SEBI Regulated Entities
Securities and Exchange Board of India, Board Meeting Proposal	India	10.4.2. Data classification and localization: To set up robust security controls for data generated / managed / processed by REs, CSCRF classifies data in two categories: 'Regulatory Data' and 'IT and Cybersecurity Data'. While 'Regulatory Data' is mandatorily localized, dispensation for 'IT and Cybersecurity Data' for offshoring has been given with suitable guardrails.	https://www.sebi.gov.in/media-and-notifications/press-releases/jun-

from June 27, 2024			2024/sebi-board-meeting_84448.html
Government Regulation 71 of 2019 regarding the Operation of Electronic Systems and Transactions	Indonesia	Summary: In October 2019, the Government of Indonesia issued Government Regulation 71 on the Operation of Electronic Systems and Transactions (GR71) to supersede and replace GR82. GR71 explicitly clarifies that public sector data must be managed, stored, and processed in Indonesia, but there is no similar restriction on private sector data, which can be managed, stored, and processed anywhere, subject to requirements with respect to financial sector data that may be imposed by the financial sector regulator. Indonesia's reflection of the broad principle in GR71 that "private electronic systems operators" may place their systems and data outside of Indonesia is a positive development. However, so-called “Public Scope Electronic System Providers” are required to store and process data onshore. Additionally, Article 99 of GR 71 states that institutions holding “Strategic Electronic Data” must hold archives and must be connected to a specific data center. “Strategic Electronic Data” encompasses data relating to energy, transportation, financial, healthcare, ICT, food, defense, and other sectors stipulated by the Government	Government Regulation 71 of 2019 regarding Operation of Electronic Systems and Transactions BSA, 2021 NTE submission USTR, 2021 NTE Report
OJK (Financial Services Authority, Regulations 13/2020 and 38/2020	Indonesia	Summary: In 2020, OJK issued Regulations 13/2020 and 38/2020, which appear to allow some but not all data to be transferred and stored outside of Indonesia for commercial banks and insurance companies. OJK has confirmed that certain categories of electronic systems, namely front-end systems including those containing individual transaction or customer details, held by banks may be stored outside of Indonesia with OJK’s approval.	USTR, 2021 NTE Report Microsoft, Financial Services in Indonesia
Financial Services Authority Regulation No. 38/POJK.03/2016 as partially amended by Financial Services Authority Regulation No. 13/POJK.03/2020 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank	Indonesia	Article 21 paragraph (2) of Financial Services Authority Regulation No. 38/POJK.03/2016 as partially amended by Financial Services Authority Regulation No. 13/POJK.03/2020 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data center or a data processing outside Indonesia territory) necessitates prior approval being obtained from the Financial Services Authority ("FSA").	DLA Piper

Finance Services Commission. Korea, Amended Electronic Financial Supervisory Regulations for Expanded Cloud Service Usage in the Finance Sector	Korea	While the Amendment allows the use of cloud services for the processing of both personal credit information and unique identification information, in order to promptly respond to service interruptions and possible accidents, financial companies and electronic financial business operators will be required to use cloud systems (including management systems) located in Korea for the processing of personal credit information and unique identification information. “Article 14-2 (Procedures for Using Cloud Computing Services, etc.) 8 The computer rooms in which the information processing system of the cloud computing service provider is located after the procedure described in Paragraph 1 shall not be applied to Article 11, No. 11, No. 12, and No. 5 of Article 15, No. 1. However, if a financial company or an electronic financial business entity (excluding the domestic branch of a foreign financial company that does not significantly affect the safety and reliability of electronic financial transactions, and an electronic payment agent for overseas cyber malls pursuant to Article 50-2) processes unique identification information or personal credit information through cloud computing services, Article 11-12 shall apply, and the relevant information processing system shall be installed in Korea. <Clued New 2018. 12. 21., Revised 2022. 11. 23.> “	Electronic Financial Supervisory Regulations (2023) Kim and Chang explanation
Credit Information Use and Protection Act, Korea	Korea	Under the Act and its subordinate regulations, financial institutions cannot delegate the processing of unique identification data (e.g., resident registration number, driving licence number, passport number, foreigner registration number) overseas. Further, if a financial institution wants to process unique identification data or personal credit information through a cloud computing service, the cloud computing system must be located in South Korea. “Article 17 (Entrustment of Processing) (1) A credit information company, etc. may entrust a third party with the business affairs of processing credit information. In such cases, Article 26 (1) through (3) of the Personal Information Protection Act shall apply mutatis mutandis to the entrusted processing of personal credit information. <Amended on Feb. 4, 2020> (2) A credit information company, etc. may entrust the processing of credit information; and Articles 19 through 21, 22-4 through 22-7, 22-9, 40, 43, 43-2, 45, 45-2, and 45-3 (including penalty provisions and provisions regarding administrative fines in relation to such Articles) shall apply mutatis mutandis to the processing of entrusted business affairs by the entrusted person (hereinafter referred to as "trustee"). <Amended on Mar. 11, 2015; Feb. 4, 2020> (3) A credit information company, etc. prescribed by Presidential Decree, which intends to entrust the processing of credit information under paragraph (2), shall notify the Financial Services Commission of the scope of the credit information provided, etc., as prescribed by Presidential Decree. (4) In providing any personal credit information to an agent in order to entrust the processing of credit information under paragraph (2), a credit information company, etc. shall take measures to protect information that can uniquely identify an individual, such as encryption, as prescribed by Presidential Decree. <Newly Inserted on Mar. 11, 2015> (5) Where a credit information company, etc. has provided any credit information to a trustee, it shall educate the trustee as prescribed by Presidential Decree to prevent the credit information from being lost, stolen, disclosed, altered, or compromised and reflect matters for the safe processing of credit information by the trustee in the entrustment contract. <Newly Inserted on Mar. 11, 2015; Feb. 4, 2020> (6) Where the trustee uses personal credit information or provides it to a third party, Article 26 (5) of the Personal Information Protection Act shall apply. <Amended on Feb. 4, 2020> (7) No agent shall further outsource any of the duties under paragraph (2) to any third party: Provided, That this shall not apply where the Financial Services Commission acknowledges within the scope not compromising the protection and safe processing of credit information. <Newly Inserted on Mar. 11, 2015>”	Credit Information Use and Protection Act, Korea
Central Bank of Nigeria,	Nigeria	Summary:	Thompson Reuters, Data

Guidelines on Point of Sale Card Acceptance Services (2011)		"Guideline 4.4.8 requires entities engaging in point of sale (POS) card acceptance services in Nigeria to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic POS and ATM transactions. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers."	Localization Laws - Nigeria
Sensitive Data Localization Rules	Pakistan	Data collated by banks, insurance firms, hospitals, defense establishments and other 'sensitive' institutions may not be transferred to any individual or body without authorization from the relevant regulator on a confidential basis. Such data is further regulated by contractual terms. In certain cases, data may not be transferred without authorization from the data subject.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PK

Ley N° 29733 - Ley de Protección de Datos Personales (in Spanish)	Peru	Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy. The Personal Data Protection Law N° 29733 (PDPL) was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP (Regulation) was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.
		
		Further, the law regulating private risk centers and the protection of the owner of the information is Law Nº 27489, enacted in 2001 and later amended several times. This law establishes the applicable provisions for activities related to risk centers and companies that handle:
		
		• Information posing higher risks to individuals (eg, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
		• Sensitive personal data (according to the PDPL)
		
		Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation. Generally, data subject consent is required.
		
		In the case of cross-border transfers, the transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels' to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:
		
		• In accordance with international treaties in which Peru is a party
		• For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
		  ○ Terrorism
		  ○ Drug trafficking
		  ○ Money laundry
		  ○ Corruption
		  ○ Human trafficking, and
		  ○ Other forms of organized crime
			https://doc.contraloria.gob.pe/documentos/Cuadro_Ley_Proteccion_Datos_Personales.pdf
			
			https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PE

		• When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship • Bank or stock transfers concerning transactions in accordance with the applicable law • The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied • The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction • Other exempt purposes established by the Regulations For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.	
SARB	South Africa	Need to know current status and get better source "2018: The South African Reserve Bank imposed a moratorium prohibiting the migration of domestic transaction volumes from Bankserv (South Africa's bank-owned domestic payment switch) to international payment schemes. The South African Reserve Bank enacted the moratorium after it found out that domestic South African banks planned to move more of their transactions to global payment service networks. The moratorium was to be in place until a new policy was developed and enacted"	https://www2.itif.org/2021-data-localization.pdf
Banking Information Systems and Electronic Banking Services Regulation (Official Gazette No. 31069, March 15, 2020)	Turkey	Summary: "The Regulation addresses the sharing and cross-border transfer of client information. Save for the exceptions under the Banking Law, banks cannot transfer or disclose to any third parties in Turkey or abroad any information that can be regarded as clients secrets that banks acquired, stored or processed through information systems during the performance of their activities and the procurement of outsourced services, without the client's request in written form, or that is verifiable through permanent data storage. Clients' explicit consent for the disclosure of personal data cannot be a precondition for the provision of the services."	Esin Law, New Regulation on Bank IT Systems and Electronic Banking Services
Communiqué on Information Systems Management numbered VII-128.9 (January 5, 2018)	Turkey	Summary: The communique imposes data localization requirements specifying that any companies subject to independent audit will be required to maintain their primary and secondary IT systems within the territory of Turkey.	Eryulekli, Communiqué published by capital markets board on information systems management Erdem & Erdem, Management of Information Systems

Banking Law No. 5411, Privacy-related Amendments (2020)	Turkey	Summary from ESIN Law: The Banking Law No. 5411 (“Banking Law”) was amended, altering banks’ data privacy practice (“Amendments“). The Amendments were published in the Official Gazette on February 25, 2020 and entered into force on the same date • Per Article 73, customer secrets may not be disclosed or transferred to any third party located in Turkey or abroad without a request or instruction from the customer, even if the explicit consent of the customer is collected in line with the Data Protection Law. The only exemptions to this rule are the mandatory legal provisions in other laws and information that must be disclosed to certain ministries listed in Article 73. • Further, the Board of the Banking Regulatory and Supervisory Authority is authorized to prohibit the transfer of customer secrets or bank secrets to third parties abroad after it assesses the customer secret’s economic security, and may render a decision ordering banks to retain their information systems and their back-ups in Turkey. • Disclosures and transfers of customer and banking secrets, including disclosures and transfers made based on the exemptions provided in the Article, must be made to the extent they are limited with the specified purposes and are proportionate. • The Board is authorized to determine the scope, method, principles and procedures related to the disclosures and transfers of customer secrets and introduce limitations related to these.	ESIN Law, Data Privacy Amendments to Turkish Banking Law