RSC 2024/21
Robert Schuman Centre for Advanced Studies
Global Governance Society

# WORKING PAPER

## Data localisation: global trends

Martina Francesca Ferracane and Simón González Ugarte

European University Institute
**Robert Schuman Centre for Advanced Studies**
Global Governance Society

# Data localisation: global trends

Martina Francesca Ferracane and Simón González Ugarte

RSC 2024/21

ISSN 1028-3625



Published in July 2024 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy



With the support of the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

**Robert Schumann Centre for Advanced Studies**

The Robert Schuman Centre for Advanced Studies (RSCAS) was created in 1992 and is currently directed by Professor Erik Jones, and it aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The RSCAS is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

**The Global Governance Programme**

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre. It is a community of outstanding professors and scholars, that produces high quality research and engages with the world of practice through policy dialogue. Established and early-career scholars work on issues of global governance within and beyond academia, focusing on four broad and interdisciplinary areas: Global Economics, Europe in the World, Cultural Pluralism and Global Citizenship. The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its executive training programme: the Academy of Global Governance, where theory and 'real world' experience meet and where leading academics, top-level officials, heads of international organisations and senior executives discuss on topical issues relating to global governance.

For more information: http://globalgovernanceprogramme.eui.eu

## Abstract

This paper provides evidence of the variety of restrictions to data transfers imposed over time across 150 countries. It presents a taxonomy of the different types of data localisation policies enriched by examples of laws implemented globally and provides aggregated statistics for these policies, highlighting sectoral and regional trends. By enhancing transparency, the paper aims to facilitate empirical research and trade policy discussions related to data flows.

## Keywords

Data flows; digital trade; digital economy; trade policy; data localisation

## Acknowledgments

We would like to thank the participants of the Roundtable on “Digital Trade and Data Governance in the Age of AI” at the Bank of Italy (June 2024) for their comments.

# Table of contents

# 1. Introduction

The Internet, as we know it today, is fundamentally dependent on open data transfers across borders. It has been designed so that data packets randomly cross borders, taking different paths that respond to technical needs to maximise efficiency and ensure integrity and availability. Yet, the growing importance of data and new concerns for privacy, security and law enforcement have led governments to constrain data transfers, imposing diverse regulations to expand their regulatory reach to the online space.

While the effectiveness of these policies to achieve their intended policy objective is still subject to debate, there is growing evidence that points to their costs for businesses. Restrictions on data flows impact the provision of services not only across borders but also within borders, requiring companies to adjust their operations to control the location where data (and their mirrored copies) are processed and stored. Equally costly are the impacts of localisation rules on international trade, and in fact, companies have consistently ranked these measures among the most costly trade restrictions.[1] The empirical evidence confirms these claims with research finding a negative effect of data flows' restrictions on GDP, trade in services, productivity, and innovation.[2]

Data localisation policies are not only associated with economic costs, they can also limit privacy and freedom of expression.[3] This is the case of measures that apply to communication, whether private communication among platform users or public information disseminated through blogs, online newspapers, and other websites. By keeping a copy of certain data locally, governments can more easily control this information and access the data to identify the creator of the content. Eventually, these policies can affect the architecture of the Internet, which was built as a distributed network of networks beyond national borders.[4]

In this paper, we aim to shed light on this phenomenon by providing evidence of the variety of restrictions to data transfers imposed over time. We rely on the data collected in the Digital Trade Integration (DTI) database hosted by the European University Institute that maps regulatory policies in 146 countries implemented until December 2023,[5] which we integrated with four additional countries from South Asia for a total of 150 countries included in our analysis.[6] We first present a taxonomy of the different types of data localisation policies enriched by different examples of laws implemented globally. We then present aggregated statistics for these policies, highlighting sectoral and regional trends, and conclude by offering a perspective on the recent debate about data localisation in trade policy.

1 N. Cory and L. Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", *Information Technology & Innovation Foundation,* 19 July 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (last accessed in March 2024); and C. Del Giovane, J. Ferencz and J. López González, "The Nature, Evolution and Potential Implications of Data Localisation Measures", OECD Publishing, Paris, OECD Trade Policy Papers, No. 278 (2023), https://doi.org/10.1787/179f718a-en.

2 M.F. Ferracane, "The Costs of Data Protectionism", in M. Burri (ed), *Big Data and Global Trade Law*, Cambridge: Cambridge University Press, 2021, pp. 63–82.

3 A. Shahbaz, A. Funk and A. Hackl, "User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization", *Freedom House*, July 2020, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty (last accessed in March 2024).

4 W. J. Drake, V. G. Cerf, and W. Kleinwächter, "Internet Fragmentation: An Overview", *World Economic Forum*, 23 January 2016, https://www.weforum.org/publications/internet-fragmentation-an-overview/ (last accessed in March 2024).

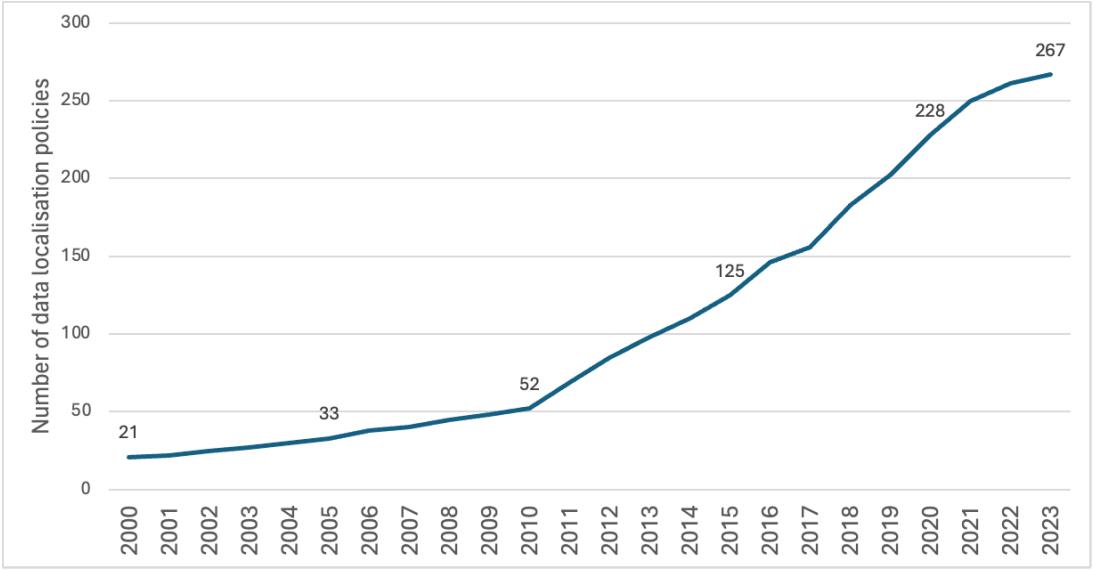
5 M. F. Ferracane (Ed.), "Digital Trade Integration Database", European University Institute *et al.,* 2022, available at https://dti.eui.eu/database/

6 The countries covered in the DTI database are: Algeria, Angola, Argentina, Australia, Austria, Bahamas, Bahrain, Barbados, Belgium, Belize, Benin, Bolivia, Botswana, Brazil, Brunei, Bulgaria, Burkina Faso, Burundi, Cabo Verde, Cambodia, Cameroon, Canada, Central African Republic, Chad, Chile, China, Colombia, Comoros, Congo, Costa Rica, Cote D'ivoire, Croatia, Cuba, Cyprus, Czech Republic, Democratic Republic Of Congo (DRC), Denmark, Djibouti, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Eswatini, Ethiopia, Finland, France, Gabon, Gambia, Germany, Ghana, Greece, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Honduras, Hong Kong, Hungary, India, Indonesia, Ireland, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Korea, Kuwait, Kyrgyz Republic, Laos, Latvia, Lesotho, Liberia, Libya, Lithuania, Luxembourg, Madagascar, Malawi, Malaysia, Mali, Malta, Mauritania, Mauritius, Mexico, Morocco, Mozambique, Myanmar, Namibia, Nepal, Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway, Oman, Pakistan, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, Rwanda, Saint Lucia, Sao Tome And Principe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Singapore, Slovakia, Slovenia, Somalia, South Africa, South Sudan, Spain, Sudan, Suriname, Sweden, Taiwan, Tajikistan, Tanzania, Thailand, Togo, Trinidad And Tobago, Tunisia, Türkiye, Turkmenistan, Uganda, United Kingdom, United States, Uruguay, Uzbekistan, Vanuatu, Venezuela, Vietnam, Zambia, Zimbabwe. The additional four countries are: Afghanistan, Bangladesh, Bhutan, and Sri Lanka.

## 2. A taxonomy of data localisation measures

Although there is no commonly agreed-upon definition for data localisation, this term generally refers to a wide range of restrictions that apply to cross-border data transfers.[7] These restrictions may take the form of any measure that raises the cost of conducting business across borders by mandating companies keep data within a certain border or imposing additional requirements for data transfer abroad. Differing widely in how they are designed and in their scope of application, they share the trait of incentivising private entities to process their data in the jurisdiction where they are located. Restrictions on cross-border data flows are not new, but they have mushroomed since 2010. Focussing on measures applied at the national level alone, the number of measures has more than quintupled from 2010 to 2023 (Figure 1).

**Figure 1: Global data localisation measures growth (2000-2023)**

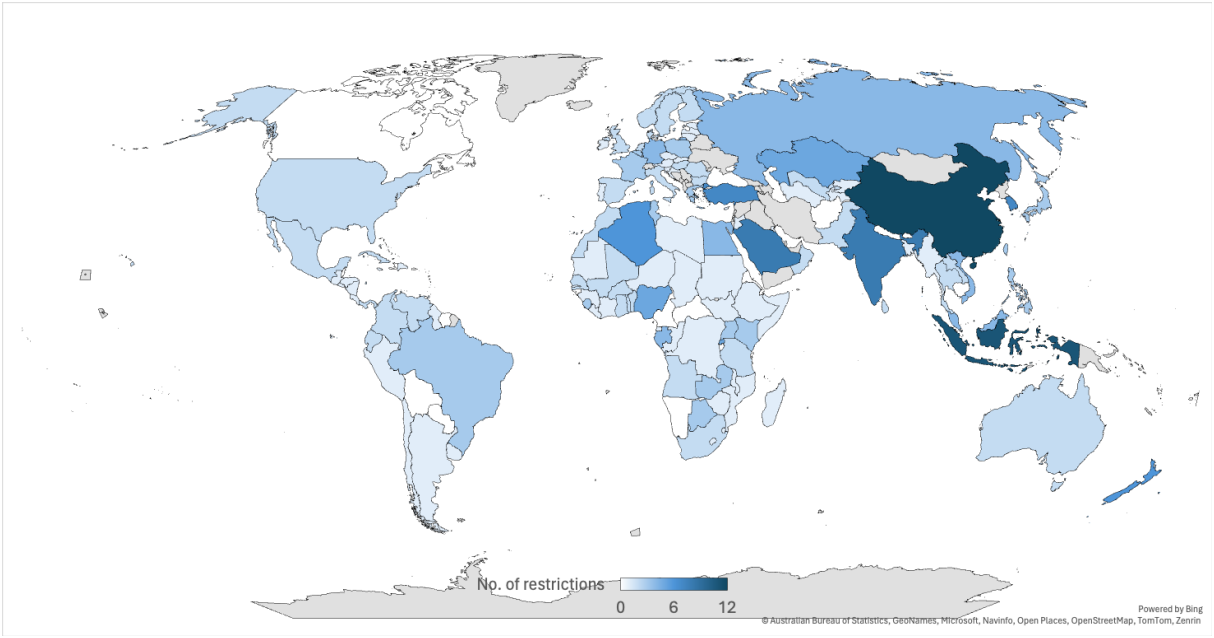



Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies. Note: we consider the year of signature of the law for the calculations.

Figure 2 provides an overview of the number of data localisation policies implemented by country. While a limited number of countries in our sample do not regulate data transfers (19 countries), two-thirds of the countries assessed have implemented one or two policies restricting data transfers across countries. Only eight countries among those assessed have implemented more than five restrictive policies on data transfers; these are China (12 policies), Indonesia (11 policies), India (8 policies), Saudi Arabia (8 policies), Republic of Korea (7 policies), Türkiye (7 policies), Algeria (6 policies), and New Zealand (6 policies). These policies are quite diverse, and their impact on trade varies depending on various factors, including the type of restriction imposed, the type of data affected, the sectors covered by the measure, and the availability of alternative data processing services in the country.

7 M. F. Ferracane, "Data Localization", in T. Cottier and K. Nadakuvaren-Schefer (eds) ,*Encyclopedia of International Economic Law*, 2nd edn (Cheltenham: Edward Elgar, 2024), 2024, available at https://www.elgaronline.com/display/book/9781800882324/IV.7.1.3.xml

**Figure 2: Number of data localisation measures per country (2023)**




Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies. The countries in grey are not covered in the analysis.

Three broad categories of restrictions can be applied to data transfers across borders. A measure does not always clearly circumscribe to one category, as the characteristics and exceptions of each policy can vary widely. Moreover, the approach followed by the European Union with its General Data Protection Regulation (GDPR),[8] which imposes the fulfilment of certain conditions for the transfers of data abroad, has become a common practice all over the world, making policies à la GDPR no longer considered as falling under the scope of trade restrictions. This is despite the conditions associated with cross-border data transfers of personal data under this model, creating costs for businesses[9] and being potentially not compliant with multilateral trade commitments.[10] For these reasons, we include these policies in the list of data localisation rules, which we categorise into three main groups: local storage requirements, conditional regimes and local processing requirements.

### *Local Storage Requirement*

When a local storage requirement applies, the data can only be transferred across borders if a copy is stored within the borders of the country imposing the requirement. As long as a copy of the data is stored domestically, data processing activities can also occur outside the country, and a business can operate as usual. This requirement usually applies to tax and accounting records, financial transactions, user data generated in the telecom sector, and corporate documents, with the objective of enabling law enforcement authorities to access data when needed. The Central Bank of Bahrain Rulebook, for example, mandates that conventional bank licensees maintain financial data on their premises in Bahrain either in its original form or as a hard copy.[11] Another example is the UK's Companies Act, which requires companies to store a copy of their accounting records must also be kept domestically.[12] In recent years, the conditional model has also emerged as an alternative to local storage requirements to ensure that certain data remains accessible for law enforcement, as shown in the next section.

8 General Data Protection Regulation (Regulation 2016/679), Chapter 5 (April 2016), available at https://gdpr-info.eu/

9 M. F. Ferracane and Van der Marel, E., "Governing personal data and trade in digital services", Special Issue Paper, Review of International Economics, 2024.

10 See e.g. C.L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", Melbourne Journal of International Law, Vol. 12, No. 1, 2011; S. Peng, "Digitalization of Services, the GATS and the Protection of Personal Data", in Sethe *et al.* (eds.), Kommunikation, Festschrift für Rolf H. Weber, 2011; R. H. Weber, "Regulatory Autonomy and Privacy Standards Under the GATS", Asian Journal of WTO & International Health Law and Policy, Vol. 7, No. 1, pp. 25-48, March 2012; and C. Kuner, "Transborder Data Flows and Data Privacy Law", *Oxford: Oxford University Press,* 2013.

11 Central Bank of Bahrain Rulebook, OM-6.3.1 (October 2011), available at https://cbben.thomsonreuters.com/rulebook/om-631-3

12 Companies Act 2006, Section 388 (November 2006), available at https://www.legislation.gov.uk/ukpga/2006/46/section/388

### *Conditional Flow Regime*

When a conditional flow regime is in place, the transfer of the data abroad is forbidden unless certain conditions are fulfilled. The conditions can apply to the recipient country, the company, or both the recipient and the company. In most of the cases, it is enough that one of the alternative options is fulfilled for the company to transfer data abroad.[13]

The European data protection regime is a typical example of a conditional regime. Under this regime, the company can transfer data abroad only to countries with an "adequate level of protection" or if the transferee fulfils certain conditions, including the use of standard contract clauses (SCCs) or binding corporate rules (BCRs). Alternatively, the data can be sent abroad if certain exceptions apply that include the data subject's consent or the necessity of the transfer for fulfilling contractual terms or for medical treatment.[14]

Applying certain conditions to transfers of personal data across borders has become a common policy worldwide. In fact, over 160 countries have implemented a data protection regime, most of which resemble the EU model.[15] Under this model, privacy protection travels with the data - protection rules continue to apply regardless of where the data is processed - also resulting in a potential clash of jurisdictions for businesses.[16] This model is considered an alternative to stricter local processing requirements, as it protects privacy while still enabling the flow of data across borders. Argentina was among the first countries to implement a law inspired by the EU model back in 2000. The law prohibits the transfer of personal data to countries or international organisations that do not provide adequate levels of protection, with some exceptions that resemble those of the 1995 Data Protection Directive of the EU.[17]

In recent years, the conditional model has also emerged as an alternative to stricter policies to ensure that certain (for example, financial) data remains accessible for law enforcement. Instead of requiring data to be stored locally, governments permit storing and processing abroad as long as it is made available to the relevant authorities when requested. An example are the Regulations No. CBL/RSD/003/2020, which provide that IT and security systems of e-payment service providers can be hosted in another jurisdiction as long as the licensed institutions ensure that the information requested is provided promptly to the authorities and that the Central Bank of Liberia has unfettered access to reports generated by the system.[18] Similarly, Hong Kong's Securities and Futures Commission released a Circular in October 2019 that requires banks and other regulated groups to store data locally or ensure that their cloud provider will hand over information on request.[19] While these policies do not impose costly conditions, we still categorise them as conditional regimes, given that they impose certain requirements on businesses.

13 If the conditions are stringent and cannot be fulfilled by the recipient country nor the company, the measure results in a ban on the transfer of data abroad.

14 GDPR, *supra* note 8. This regime is in place in the since 1995, with the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 - 0050.

15 G. Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills", *The University of New South Wales Faculty of Law Research Series,* 10 February 2023, http://www8.austlii.edu.au/cgi-bin/viewdb/au/journals/UNSWLRS/ (last accessed in March 2024).

16 S. Kolo ßa, "The GDPR's Extra-Territorial Scope: Data Protection in the Context of International Law and Human Rights Law", Zeitschrift Für Ausländisches Öffentliches Recht und Völkerrecht (2020) Nr. 4, S. 791-818.

17 Personal Data Protection Act (Act No. 25.326 of 2000), Art. 12 (October 2000), available at https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion, Directive 95/46/EC, *supra* at 14.

18 Regulations Concerning the Licensing & Operations of Electronic Payment (E-Payment) Services (No. CBL/RSD/003/2020), The Liberia Official Gazette, Regulation 9.0 (January 2020), available at https://www.cbl.org.lr/sites/default/files/documents/Licensing_Operations_E_Payment_1.pdf

19 Circular to Licensed Corporations - Use of external electronic data storage (October 2019), available at https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59

### *Local Processing Requirement*

When a local processing requirement applies, data processing must be performed locally. Therefore, the company needs to switch to local providers of data processing solutions or use its data centres located in the country to conduct the data processing data. This regime can take different forms, depending on whether the requirement applies to the main processing or any processing of certain data, and whether there are exceptions that enable businesses to conduct processing abroad.

In some cases, after the main data processing is conducted locally, the company can send the data abroad without additional limitations. This can be important for lag-free communication between subsidiaries or data security, and in fact, some countries are revising their regulation to enable transfers. This is the case, for example, of the Venezuelan Decree No. 1.402 on Banking Sector Institutions. The Decree prohibits banking institutions from transferring their main computer centres and databases to foreign territories, whether in electronic form or as physical documents belonging to users, but they are free to choose the location of their secondary computer centres and databases.[20] The repealed Banking Sector Institutions Law of 2010, on the other hand, prohibited the transfer of all computer centres and databases and not only those determined to be principal, therefore imposing a stricter restriction.[21]

Stricter requirements to conduct all data processing in the country are rare and usually apply to specific sets of especially sensitive data, such as health or public sector data, or only on transfers to specific countries for political reasons. The Zambian Data Protection Act provides a clear example of this case requiring that sensitive personal data must be processed and stored within the country in a server or data centre.[22] Similarly, the Tunisian Decree-Law No. 2-2022 forbids companies from transferring their databases with credit information activities outside Tunisia or hosting them in the cloud.[23] We also find a *de facto* ban in Pakistan, which reportedly prohibits data transfers to certain places it does not recognise, such as Armenia, Israel, and Taiwan.[24] In these cases, a local processing requirement does not allow the company to send a copy of its data abroad even after the main processing occurs in the country. Therefore, data must be stored, processed, and accessed within the territory of the implementing country with virtually no exceptions.

In some cases, the companies must request permission from the authorities to conduct the main or secondary data processing abroad in limited circumstances. These requirements are usually associated with national security and public order concerns and applied to “important” or “critical” data, although they also apply to personal data in certain jurisdictions. Sometimes, the companies must request ex-ante authorisation to send a copy of their data abroad. A well-known example is China's Cybersecurity Law, which requires “key information infrastructure” operators to store personal information and critical data within China unless there is a genuine business need. In such cases, a “security assessment” must be conducted following procedures formulated by the Cyberspace Administration of China (CAC) in collaboration with other authorities.[25] This is also the case in several African economies, including Tunisia, where, in addition to requiring ex-ante authorisation, the companies must also comply with certain conditions, including the adequacy of the recipient country, to process personal data abroad.[26]

20 Decree No. 1.402, enacting the Decree with Rank, Value and Force of Law on Banking Sector Institutions, Official Gazette of the Bolivarian Republic of Venezuela, Art. 97(8) (November 2014), available at https://www.asambleanacional.gob.ve/storage/documentos/leyes/decreto-n0-1402-mediante-el-cual-se-dicta-el-decreto-con-rango-valor-y-fuerza-de-ley-de-instituciones-del-sector-bancario-20211026183241.pdf

21 The 2010 Law was reformed in 2011 by Decree 8.079, which maintained the restriction in Art. 99. This 2011 Decree was repealed by Decree No. 1.402 of 2014.

22 Data Protection Act, 2021 (No. 3 of 2021), Section 70(3) (March 2021), available at https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

23 Decree-Law No. 2-2022, Organising the Activity of Credit Information, DCAF - Geneva Centre for Security Sector Governance, Art. 21 (January 2022), available at https://legislation-securite.tn/latest-laws/decret-loi-n-2022-2-du-4-janvier-2022-portant-organisation-de-lactivite-du-renseignement-de-credit

24 DLA Piper, “Data Protection Laws of the World |Pakistan|”, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=PK (last accessed 14 March 2024).

25 Cybersecurity Law, Art. 37 (November 2016), available at https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

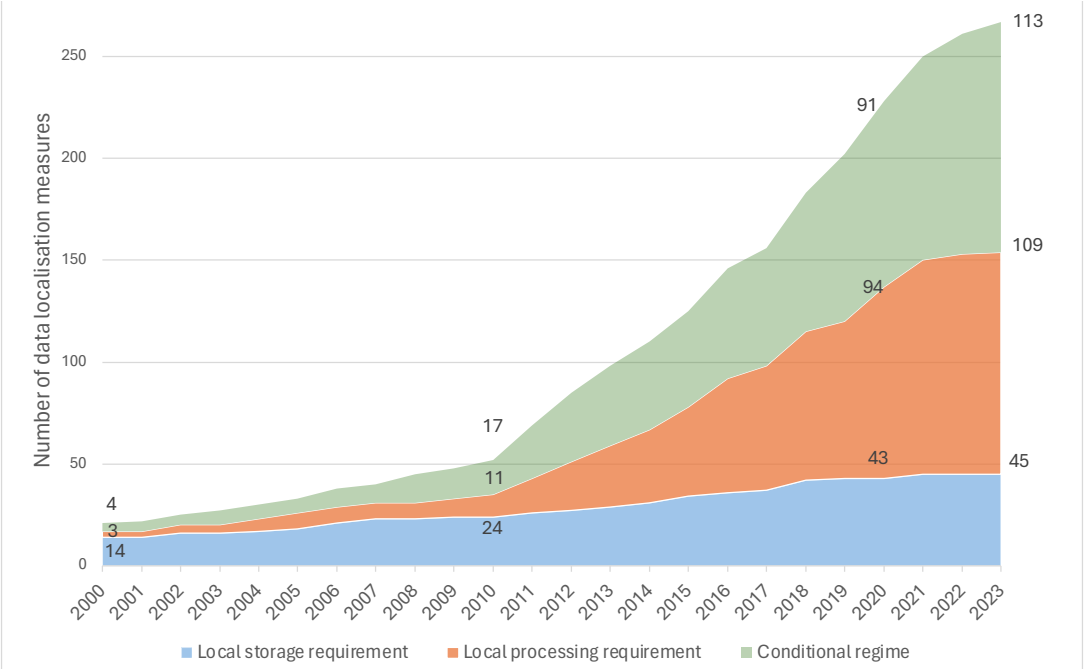
26 Organic Act No. 2004-63 on the Protection of Personal Data, Arts. 50-52 (July 2004), available at http://www.inpdp.nat.tn/ressources/loi_2004.pdf

Finally, there are instances in which a local processing requirement is associated with the need to use (and sometimes even build) a specific data centre or a server in the country. An example can be found in Kazakhstan,[27] where operators of communication networks must create - at their own expense - a system of centralised management of their networks, which must be located on the territory of the Republic of Kazakhstan. Also, Algerian Decision No. 48/SP/PC/ARPT/17 requires cloud computing service providers to establish their infrastructure on national territory using the latest and most reliable equipment and provide services through specifically declared infrastructures.[28] In Indonesia, financial companies and crypto operators have to build disaster recovery centres to ensure activity continuity in case of natural disasters.[29]

## 3. Global trends

Restrictions on cross-border transfers have increased significantly over time, especially in the last decade (Figure 3). Since 2010, local processing requirements have increased more than nine-fold, conditional flow regimes have increased more than six-fold, and local storage requirements have almost doubled.

**Figure 3: Number of data localisation measures by category (2000-2023)**




Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts. Note: we list regimes that include both a local processing requirement and additional conditions in the category of local processing.

In 2023, conditional regimes are the most common measures, accounting for 42% of all restrictions. This is largely due to the 'Brussels effect', with more and more countries adopting a data protection regime similar to the European Union.[30] Once prevalent at the turn of the century, local storage requirements are now the least common, accounting for 17% of all measures, while local processing requirements make up 41% of the policies.

27 Law of the Republic of Kazakhstan No. 567-II About communication, Institute of legislation and legal information of the Republic of Kazakhstan of the Ministry of Justice of the Republic of Kazakhstan, Art. 21 (July 2004), available at https://adilet.zan.kz/eng/docs/Z040000567_

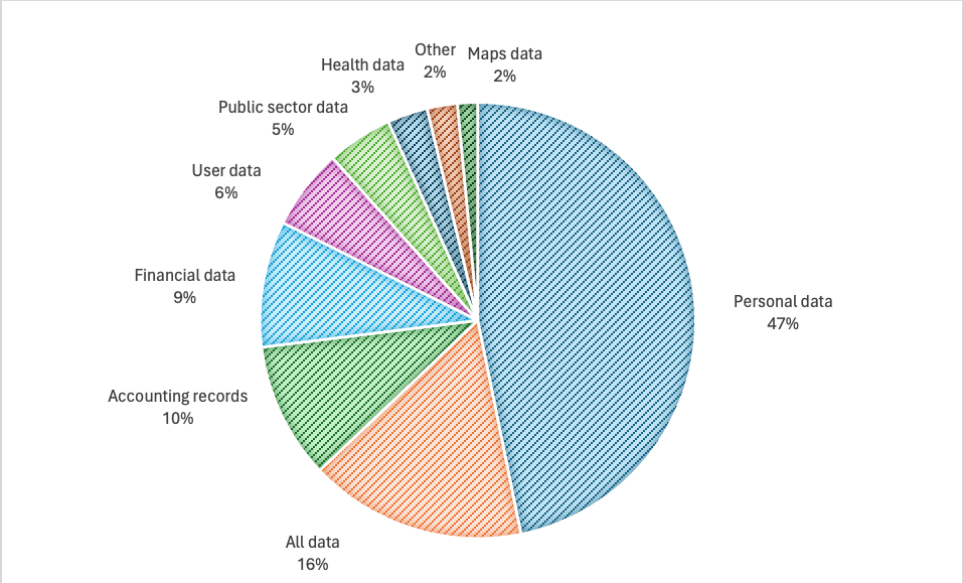
28 Decision No. 48/SP/PC/ARPT/17 defining the conditions and modalities for establishing and operating of hosting and storage services for computerised content for user benefit in the context of cloud computing services, Art. 10 (November 2017), available at https://www.arpce.dz/fr/file/m3k5e0

29 Regulation No. 4/POJK.05/2021 - Implementation of Risk Management in the Use of Information Technology by Nonbank Financial Services Institutions, Art. 23 (March 2021), available at https://peraturan.go.id/files/ojk4-2021bt.pdf and Regulation No. 8 of 2021 on Implementing Guideline of Physical Market Trading of Crypto Assets in the Futures Exchange, Arts. 7, 11, 14 and 18 (October 2021), available at https://bappebti.go.id/pbk/sk_kep_kepala_bappebti/detail/8952

30 A. Bradford, "The Brussels Effect: How the European Union Rules the World", Oxford University Press, 19 December 2019, available at https://doi.org/10.1093/oso/9780190088583.001.0001

Nearly half of all policies aim to apply to personal data transfers (Figure 4), typically through comprehensive data protection legislation that applies horizontally to all sectors, imposing conditions on data transfers. Yet, we also find some stricter policies that apply to personal data, as is the case in Russia's data protection law, which requires all collected data to be placed in a primary database located within the country and mandates that any operations on the data be performed locally, although data can be transferred to secondary databases abroad for further processing.[31] Box 1 provides an overview of the three alternative models that have emerged to regulate the cross-border transfers of personal data and a classification of countries based on these models.

**Figure 4: Global data localisation measures by data type (2023)**




Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies.

Some measures instead apply to all data handled by private companies in certain sectors. For instance, the Saudi Communications, Space and Technology Commission requires IoT service licensed providers and Indoor IoT network implementers to host all servers used in providing IoT services and store all data within Saudi Arabia.[32] In the US, Team Telecom, an informal grouping of the Departments of Defence, Homeland Security and Justice, and the Federal Bureau of Investigation, reportedly requires, through security agreements and assurance letters, data to be stored locally or that copies of the data be made available by telecom companies as a condition for granting a licence or consent for certain mergers or acquisitions.[33]

Around 10% of the measures, mostly local storage requirements, apply to accounting records. Most of these measures are implemented to facilitate access to these data to enforcement authorities. However, as mentioned above, several of these measures have been amended to enable businesses to process data abroad as long as they guarantee access to the authorities when requested. In Barbados, a law dating back to 1965 still requires businesses to maintain within the country records and books of account, including an annual inventory,[34] while a similar requirement that applied in New Zealand has been amended to allow for business records to be stored outside the country, provided that the company meets certain data integrity and access criteria.[35]

31 Federal Law of the Russian Federation No. 152-FZ About personal data, Art. 18(5) (July 2006, as amended in July 2014), available at http://www.kremlin.ru/acts/bank/24154/page/1

32 Internet of Things (IoT) Regulatory Framework, Section 7 (September 2019), available at https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

33 A. Bonner, C. Sechrest, J. Veach, K. Bressie, M. Nilsson and P. Caritj, "In brief: telecoms regulation in USA", *Lexology,* 14 June 2019, available at https://www.lexology.com/library/detail.aspx?g=9e7ab642-d7f6-43ed-814b-4025b62cbeaf (last accessed in March 2024).

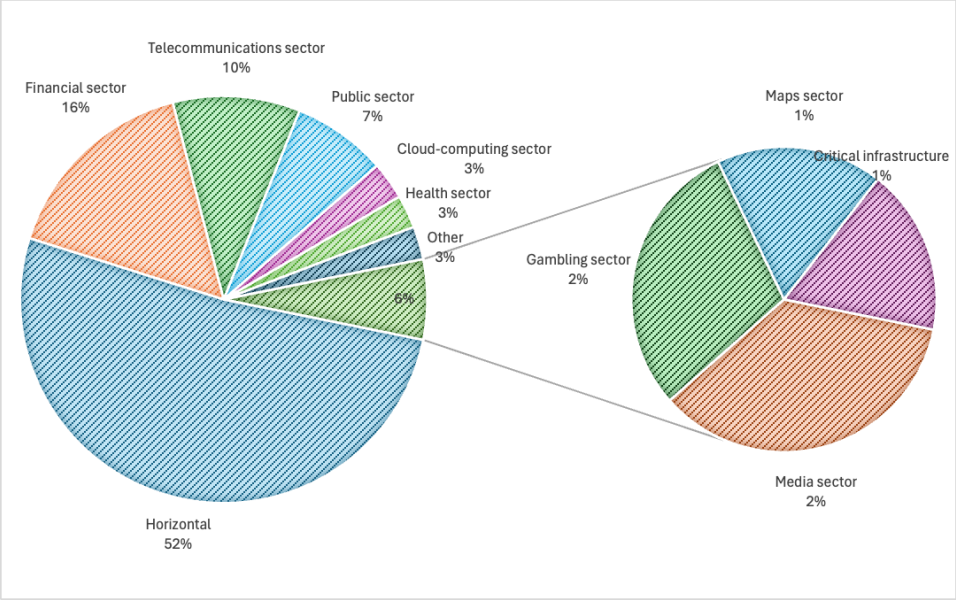
34 Income Tax Act, Section 75.1 (January 1969), available at http://barbadosparliament-laws.com/en/showdoc/cs/73/ga:l_iii-gb:l_ab#anchorga:l_iii-gb:l_ab

35 Tax Administration Act, Section 22 (December 1994, as amended in November 2012), available at https://www.legislation.govt.nz/act/public/1994/0166/latest/DLM350462.html

Policies that apply to user data usually pertain to the behaviour of users online and typically apply to telecom operators. These policies can be invasive of users' privacy and, in fact, in 2014, the Court of Justice of the European Union declared the Directive on Data Retention invalid, which required telecom operators to retain a copy of certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism.[36] However, not all national laws that implemented the Directive have been overturned. In Poland, for example, telecommunications providers are still required to keep a copy of certain types of user data locally for 12 months, including user identity, date and time, and the type of connection.[37] This requirement is even broader than the original text of the Directive, as user data must also be stored locally.

Regarding the sectoral coverage of the policies, more than half of them affect all sectors horizontally, as is the case for data protection policies and measures related to accounting records (Figure 5). Some measures apply both to all data and all sectors, as in the case of Cuban legislation, which deems it an ICT-related violation to host a site on servers located in a foreign country unless it is a mirror or replica of the main site on servers located in national territory.[38] 16% of the entries apply to the financial sector, either to all data or to personal information in this sector, while 10% of the measures apply to the telecom sector, mostly to user data.

**Figure 5: Global data localisation measures by sector (2023)**




Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies.

A recent trend is the implementation of measures that apply to "critical infrastructure", which is defined more or less broadly depending on the country implementing the policy. For instance, in Morocco, restrictions on data processing apply to companies engaging in activities related to the production or distribution of goods and services that are essential for satisfying the basic needs of the population or maintaining the country's security capacities.[39] In Zambia, data localisation provisions apply to critical information infrastructure, defined as any infrastructure that contains

36 Data Retention Directive (Directive 2006/24/EC), Art. 6 (March 2006), available at https://eur-lex.europa.eu/eli/dir/2006/24/oj. The Directive was declared invalid by Court of Justice of the European Union Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others (April 2014), available at https://curia.europa.eu/juris/documents.jsf?num=C-293/12.

37 Telecommunications Act, Arts. 180a-180c (July 2004), available at https://www.uke.gov.pl/gfx/uke/userfiles/m-pietrzykowski/telecommunications_act_en.pdf

38 Decree-Law 370/2018 on the informatization of society, Official Gazette of the Republic of Cuba, Art. 68(f) (December 2018), available at https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-o45.pdf

39 Decree No. 2-15-712 on the Protection of Sensitive Information Systems and Infrastructures of Vital Importance, Art. 9 (March 2016), available at https://www.rcar.ma/uploads/textes_de_loi/D%C3%A9cret%20protection%20des%20SI%20sensibles%20et%20infra%20vitales.pdf

any information that the Ministry declares as critical due to its importance in protecting Zambia's national security, economy, or social well-being.[40] In Saudia Arabia, the Essential Cybersecurity Controls (ECCs) apply strict localisation requirements to governmental and semi-governmental bodies in the Kingdom, as well as private entities that own, operate, or host critical national infrastructures, defined as the assets (i.e., facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in (i) significant negative impact on the availability, integration or delivery of basic services, including services that could result in a serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts; (ii) significant impact on national security and/or national defence and/or state economy or national capacities.[41]

### Box 1: Data restrictions applied to cross-border transfers of personal data

At the global level, three main regulatory models have emerged to regulate the cross-border transfers of personal data models: an open model characterised by the absence of restrictions on cross-border data flows; a conditional model characterised by the presence of certain conditions for the transfer of personal data across borders to be fulfilled ex-ante by the recipient country or the company; and a control model based on the local processing of data with strict conditions for data transfers (Table 1).[42]

**Table 1: Main features of data models on cross-border data transfers**

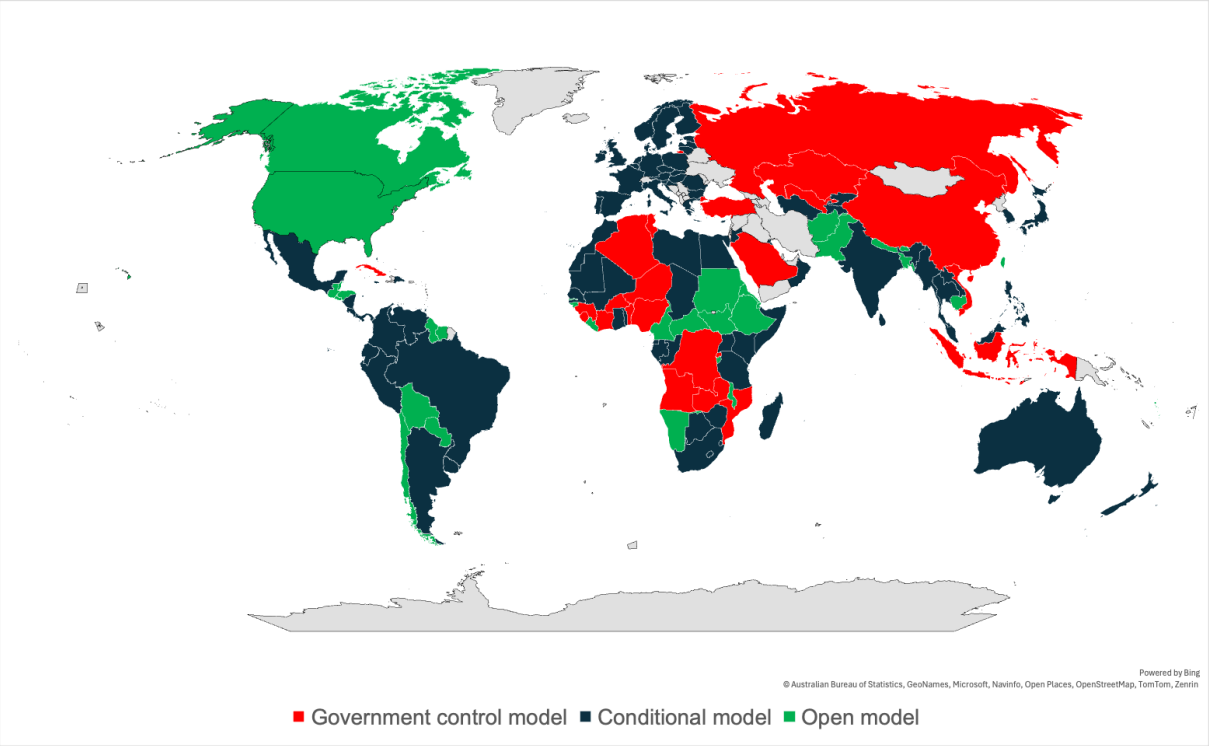
| | |
|---|---|
| **Open model** | Self-certification; self-assessment schemes; ex-post accountability; trade agreements, and plurilateral/bilateral arrangements are the only means to regulate data transfers. |
| **Conditional model** | Conditions to be fulfilled ex-ante, including the adequacy of the recipient country, binding corporate rules (BCR), standard contract clauses (SCCs), data subject consent, and codes of conduct, among other conditions. |
| **Control model** | Strict conditions, including bans on transferring data across borders; local processing requirements: ad hoc government authorisation for data transfers; infrastructure requirements; and ex-ante security assessments. |

Source: Ferracane and van der Marel (2024).

The conditional model is the most prevalent globally for regulating personal data (Figure 6). The European Union advocates this model in its GDPR,[43] and before in its 1995 Directive for Data Protection, which established an international benchmark for data protection regulation. This model has exerted such an influence globally that scholars use the term “Brussels effect” to define this phenomenon.[44] As of December 2023, 92 of the 150 countries assessed (that is, 61%) have implemented a conditional flow model, while 23 countries (15%) have implemented a control model. The remaining 23% of countries do not impose any restrictions on transferring personal data, therefore having an open model. As a result, the global data policy landscape is fragmented but dominated by the conditional model. Some trends are visible at a glance. Developed countries generally implement a conditional model, except for North America. The control model is more common in Asia and Africa, with Cuba being the only Latin-American economy implementing this model for personal data.

40 Cyber Security and Cyber Crimes Act, Section 18 (March 2021), available at https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf
41 Essential Cybersecurity Controls (ECC - 1 : 2018), Section 4.2.3.3 (2018), available at https://nca.gov.sa/ecc-en.pdf
42 Ferracane and van der Marel (2024), *supra* note 9.
43 General Data Protection Regulation, *supra* note 8.
44 Bradford (2019), *supra* note 30.

**Figure 6: Global regulatory landscape for governing personal data (2023)**

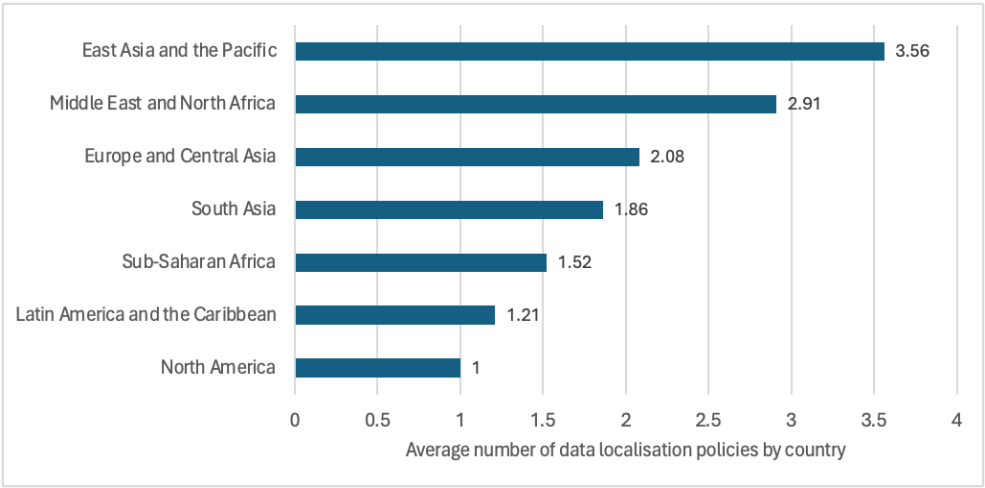



Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies. We consider the latest model applicable to each country based on the laws signed by December 2023. A previous version of this graph was published in Ferracane and van der Marel (2024).

## 4. Regional trends

Figure 7 shows the average number of data localisation measures for the 150 countries in our sample.[45] We find that the East Asia and the Pacific (EAP) countries impose the highest number of restrictive policies on average, followed closely by the Middle East and North Africa (MENA) region. North America is the least restrictive region.

**Figure 7: Average number of data localisation measures by region (2023)**




Source: Authors based on data from the Digital Trade Integration (DTI) database and additional legal texts for 150 economies.

45 We classify countries based on the World Bank official classification, available at https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups (last accessed in March 2024). Although Malta is part of the MENA region in the World Bank classification, we have listed it in the ECA region given that it is part of the EU27.

### *East Asia and the Pacific (EAP) region*[46]

Countries in the EAP region impose, on average, more than three data transfer restrictions, making up about a quarter of all measures in our sample. Of the 64 measures in the region, 28 are local processing requirements (44% of all measures), and seven are local storage requirements (11%). The remaining 29 measures are conditional regimes, mostly applied to personal data in line with the EU model.

Three out of four global measures related to map information are located in the region. One example is the Korean requirement for approval of the Minister of Land, Infrastructure and Transport to transfer map data across borders.[47] These policies, as many other local processing requirements implemented in the region, are justified on the grounds of national security.[48] For instance, a recent instrument related to the aforementioned Chinese Cybersecurity Law states that a security assessment is required before a transfer abroad can occur in four situations, one of which is when the transfer concerns "important data".[49] This term is broadly defined as data that could endanger national security, economic operations, social stability, public health, and safety. The assessment covers various aspects, such as the risks that the transfer may pose to national security or public interests, among other policy objectives.[50]

In addition to the Cybersecurity Law, China implements several data policies intending to control data transfers for different sectors and types of data. The sectors directly impacted include the telecom sector, the financial sector, the health sector, operators of critical infrastructure, maps services, and services for taxi online booking. Moreover, the country has approved in 2021 its first comprehensive data protection legislation, which requires data to be stored in the country unless the company complies with some strict conditions.[51]

In Indonesia, we find a unique type of restriction led by law enforcement concerns with specificities connected to the risk of natural disasters. The country requires companies to store data locally and, in addition, build disaster recovery centres for financial companies and crypto operators to ensure activity continuity in case of natural disasters.[52] Until 2019, the country imposed this requirement also on public electronic system operators (ESOs), which include both public bodies and entities appointed by public bodies to operate electronic systems on their behalf, effectively affecting many private sector companies. This requirement was lifted in 2019, although public ESOs are still required to manage, process, and/or store electronic systems and electronic data in the territory of Indonesia, except if the technology is not yet available.[53]

46 The following countries were analysed: Australia, Brunei Darussalam, Cambodia, China, Hong Kong, Indonesia, Japan, Korea, Lao PDR, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, Taiwan, Thailand, Vanuatu, and Vietnam.

47 Act on the Establishment, Management, etc. of Spatial Data (Act No. 12738), Art. 16 (June 2014), available at https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=228499&ancYd=20210112&ancNo=17893&efYd=20220113&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202&ancYnChk=0#

48 E. Yayboke, C. Ramos, and L. Sheppard, "The Real National Security Concerns over Data Localization", *Center for Strategic & International Studies*, 23 July 2021, https://www.csis.org/analysis/real-national-security-concerns-over-data-localization (last accessed in March 2024).

49 Cybersecurity Law, *supra* note 25.

50 Outbound Data Transfer Security Assessment Measures, Arts. 4 and 8 (July 2022), available at http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

51 Personal Information Protection Law, Art. 40 (August 2021), available at https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

52 Regulation No. 4/POJK.05/2021 and Regulation No. 8 of 2021, *supra* note 29.

53 Government Regulation of the Republic of Indonesia No. 71 of 2019 on the Organization of Electronic Systems and Transactions revoked the previous regulation, Government Regulation of the Republic of Indonesia No. 82 of 2012. Both regulations can be accessed at https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

### *Europe and Central Asia (ECA) region*[54]

As noted above, the European Union has been at the forefront of the global trend towards implementing comprehensive data protection legislation that restricts the transfer of personal data abroad, allowing it only if certain conditions are met.[55] Most of the economies in the ECA region implement policies inspired by the EU model, both among neighbouring countries such as the UK[56] and Norway,[57] and in the former Soviet Union countries, as is the case of Kazakhstan[58], the Kyrgyz Republic,[59] the Russian Federation,[60] Tajikistan,[61] Turkmenistan,[62] and Uzbekistan.[63] However, it is worth noting that in the last decade, three of these countries have amended their data protection laws to include stricter local processing requirements: Kazakhstan, in Art. 12; the Russian Federation, in Art. 18; and Uzbekistan, in Art. 27-1. Türkiye also follows the EU model for transfers of personal data across borders,[64] but it also implements several additional restrictions on subsets of personal data. For example, the Decision on E-Call Services in Vehicles, whose scope was expanded by the Decision on Remote Programmable eSIM technologies, requires that personal data related to devices utilising eSIM technology must be processed in the country, adding that the relevant modules of eSIMs are expected to be programmable only by local mobile operators and only local mobile operator profiles may be installed.[65]

In this region, we also find several local storage requirements for accounting records, most of which predate the digital era. These include the Swedish Accounting Act, which requires accounting records to be stored in the country for seven years.[66] Since the beginning of the 21st century, additional restrictions on other data types have been implemented in specific sectors, such as telecommunications, public sector, health, finance, and gambling, throughout Europe. In relation to the gambling sector, it is interesting to notice that data processing restrictions have only been implemented in the ECA region. An example is the requirement by the Malta Gaming Authority to implement real-time replication in a local server of "regulatory data" composed of player details, financial transactions, and game-play transactions.[67]

54 The following countries were analysed: 27 Member States of the European Union, Kazakhstan, Kyrgyz Republic, Norway, Russian Federation, Tajikistan, Türkiye, Turkmenistan, United Kingdom, and Uzbekistan. Although Malta is part of the MENA region in the World Bank classification, we have listed it in the ECA region given that it is part of the EU27.

55 General Data Protection Regulation, *supra* note 8.

56 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), Arts. 44-49 (April 2016), available at https://www.legislation.gov.uk/eur/2016/679/chapter/V and Data Protection Act 2018 (May 2018), available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

57 Law on the Processing of Personal Data (Personal Data Act) (June 2018), available at https://lovdata.no/dokument/NL/lov/2018-06-15-38

58 Law of the Republic of Kazakhstan No. 94-V on Personal Data and Its Protection, Institute of legislation and legal information of the Republic of Kazakhstan of the Ministry of Justice of the Republic of Kazakhstan, Art. 16 (May 2013, as amended in December 2017), available at https://adilet.zan.kz/eng/docs/Z1300000094

59 Law of the Kyrgyz Republic No. 58 About information of personal nature, Art. 25 (April 2008), available at https://cbd.minjust.gov.kg/202269/edition/1239270/kg

60 Federal Law of the Russian Federation No. 152-FZ About personal data, Art. 12 (July 2006), available at http://www.kremlin.ru/acts/bank/24154/page/1

61 Law of the Republic of Tajikistan No. 1537 About personal data protection, Art. 18 (August 2018), available at http://mmk.tj/system/files/Legislation/1537_TJ.doc.pdf

62 Law of Turkmenistan No. 519-V About Information on Private Life and its Protection, Art. 17 (March 2017), available at https://minjust.gov.tm/hukuk/merkezi/hukuk/264

63 Law of the Republic of Uzbekistan No. ZRU-547 About personal data, The National Center of Legal Information "Adolat" under the Ministry of Justice of the Republic of Uzbekistan, Art. 15 (July 2019), available at https://lex.uz/docs/4831939

64 Law No. 6698 on Protection of Personal Data, Art. 9 (April 2016), available at https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

65 Decision No. 2018/DK-YED/27 (January 2018), available at https://www.btk.gov.tr/uploads/boarddecisions/112-tabanli-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanli-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf and Decision No. 2019/DK-TED/053 (February 2019), available at https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf

66 Accounting Act (1999:1078), Chapter 7, Section 2§ (December 1999), available at https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078

67 Technical Infrastructure hosting Gaming and Control Systems Guidelines, Guideline 3.2 (December 2015), available at https://www.mga.org.mt/app/uploads/Technical-Infrastructure-hosting-Gaming-and-Control-Systems-%E2%80%93-Remote-Gaming-1.pdf

### *Latin America and the Caribbean (LAC) region*[68]

Countries in the LAC region do not impose generally strict conditions on data transfers. Most countries have implemented data protection rules in line with the European Union, while some are in the process of developing these policies. This is the case of countries in the Northern Triangle of Central America, consisting of El Salvador, Guatemala, and Honduras, which all have recently published draft laws with conditional regimes.[69] In the case of El Salvador, however, the draft was vetoed by the President in 2021.[70] In the Caribbean, several countries lack comprehensive data protection laws, including Guyana, Suriname, Haiti, and Venezuela. In the case of Venezuela, a conditional regime for personal data transfer has been established by Judgment No. 1318 of the Supreme Court of Justice.[71]

Cuba's first general data protection law came into effect in 2023, imposing stringent limitations on data transfer. Personal data can be transferred abroad only in limited circumstances or with the approval of certain government authorities.[72] Cuba is more generally characterised by a strict regime of control of the online world. An additional set of policies bans the use of foreign servers to host websites.[73] Art. 82 of Decree No. 360/2019 clarifies that when, due to connectivity needs or other interests, the entity requires hosting a site on servers located in a foreign country, this is done as a mirror or replica of the main site on servers located in Cuba, and the required measures are established to guarantee their security, in particular during the process of updating the information".

### *Middle East and North Africa (MENA) region*[74]

Most countries in the MENA region have recently implemented data protection laws based on the EU model. Bahrain,[75] Egypt,[76] Jordan,[77] Oman,[78] and Saudi Arabia,[79] have joined Morocco, which was the first country to do so in 2009.[80] However, stricter requirements are implemented in the region for public security and the state's vital interests. Algeria and Tunisia, for instance, prohibit the international transfer of personal data if it is likely to have an impact on the security of the country.[81] In addition, this region is characterised by data policies that target the media sector and media content. An example can be found in Algeria, where online information activity must be published through an electronic site hosted exclusively in Algeria, both physically and logically, with a ".dz" domain name extension.[82]

68 The following countries were analysed: Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Lucia, Suriname, Trinidad and Tobago, Uruguay, and Venezuela.

69 Greenleaf, *supra* note 15.

70 Veto to Legislative Decree No. 875 (May 2021), available at https://www.transparencia.gob.sv/institutions/capres/documents/449989/download

71 Constitutional Chamber of the Supreme Court of Justice Judgement No. 1318, safety and confidentiality principle (No. 7) (August 2011), available at http://historico.tsj.gob.ve/decisiones/scon/agosto/1318-4811-2011-04-2395.HTML

72 Law 149/2022 on Personal Data Protection, Official Gazette of the Republic of Cuba, Arts. 65- 66 (August 2022), available at https://www.gacetaoficial.gob.cu/sites/default/files/goc-2022-o90_0.pdf

73 Decree-Law 370/2018 on the informatization of society, *supra* note 38, and Decree No. 360/2019 On the Security of Information and Communication Technologies and the Defense of National Cyberspace, (May 2019), available at https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-o45.pdf

74 The following countries were analysed: Algeria, Bahrain, Egypt, Jordan, Kuwait, Libya, Morocco, Oman, Saudi Arabia, and Tunisia. Although Malta is included in this geographical group in the World Bank classification, we have listed it in the ECA region given that it is part of the EU27.

75 Law No. 30 of 2018 with Respect to Personal Data Protection Law, Arts. 12-13 (July 2018), available at http://www.pdp.gov.bh/en/regulations.html

76 Resolution No. 151 of 2020 approving the Law on the Protection of Personal Data, Chapter 7 (July 2020), available at https://mcit.gov.eg/Upcont/Documents/Reports%20and%20Documents_1232021000_Law_No_151_2020_Personal_Data_Protection.pdf

77 Personal Data Protection Law (Law No. 24 of 2023), Art. 15 (September 2023), available at https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf

78 Royal Decree 6/2022 promulgating the Personal Data Protection Law, Art. 23 (February 2022), available at https://www.mjla.gov.om/legislation/decrees/details.aspx?Id=1397&type=L

79 The Personal Data Protection Law, issued pursuant to Royal Decree No. M/19, Art. 29 (September 2021), available at https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

80 Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data, Arts. 43-44 (February 2009), available at http://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf

81 Law No. 18-07 Relating to the Protection of Individuals in the Processing of Personal Data, Art. 44 (June 2018), available at https://www.joradp.dz/FTP/JO-FRANCAIS/2018/F2018034.pdf and Organic Act No. 2004-63 on the Protection of Personal Data, *supra* note 26.

82 Decree Governing the Electronic Press (Decree No. 20-332), Art. 6 (November 2020), available at https://webservices.dz/images/pdf/F2020070.pdf

### *North America (NA) region*[83]

The Brussels effect has not yet impacted policies on personal data transfer in North America, although both Canada and the US have adequacy regimes in place for transfers of data from the European Union. The US does not have a comprehensive federal law for data protection and does not restrict the international transfer of personal data, although some state laws contain relevant provisions. Canada, on the other hand, has comprehensive legislation, but the regime differs from that found in the GDPR as the data can be transferred freely as long as the transferring organisation remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation, using contractual or other means.[84]

Additional policies can also be found at the provincial level. For instance, some provincial statutes that regulate personal health information have restrictions on its transfer outside of Canada or a specific province.[85] Some additional restrictions are found in the United States in the public sector. For example, cloud computing service providers to the US Department of Defense (DoD) may be required to store data relating to the DoD within the country. The service provider's authorising official may authorise storage of such data outside of the US, but this will ultimately depend on the sensitivity of the data in question.[86] Similarly, the US requires agencies with "specific data location requirements' to include contractual obligations identifying where 'data-at-rest […] shall be stored".[87]

### *Sub-Saharan Africa (SSA) region*[88]

Starting from 2010, there has been significant regulatory action in the SSA region to regulate personal data. As of 2023, a conditional flow model similar to the EU model had been applied by 23 countries. The latest of these measures was implemented in December 2023 in the Seychelles.[89] Yet, many of the countries have implemented stricter conditions than those of the EU model, requiring additional authorisation by certain government authorities for data transfers, as in the case of Côte d'Ivoire, which requires prior authorisation from the data protection body for personal data transfers.[90]

In the SSA region, we also find several infrastructure requirements imposing on operators to use certain facilities located in the country for data processing. For example, in Gabon, electronic communication network operators are required to have an operational management centre for their infrastructure within the national territory,[91] and in Tanzania, payment system providers are required to place their primary data centre in relation to payment system services in the country.[92]

83 The following countries were analysed: Canada and the United States.

84 Personal Information Protection and Electronic Documents Act, Justice Laws Website, Principle 4.1.3 of Schedule 1 (2000), available at https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-7.html#h-417659

85 We do not include policies implemented at the regional level in our list. For an overview of these policies in Canada, see E. Gratton, F. Joli-Coeur and S. Du Perron, "Canada - Data Transfers", *DataGuidance*, February 2024, https://www.dataguidance.com/notes/canada-data-transfers (last accessed in March 2024).

86 Code of Federal Regulations, §239.7602-2 of Part 239 of Chapter 2 of Title 48 (August 2015), available at https://www.ecfr.gov/current/title-48/chapter-2/subchapter-F/part-239/subpart-239.76/section-239.7602-2

87 Federal Risk and Management Program Control Specific Contract Clauses, Section 2.1 (December 2017), available at https://www.fedramp.gov/assets/resources/documents/Agency_Control_Specific_Contract_Clauses.pdf

88 The following countries were analysed: Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Central African Republic (CAR), Chad, Comoros, Congo, Côte d'Ivoire, Democratic Republic of Congo (DRC), Djibouti, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Uganda, Zambia, and Zimbabwe.

89 Data Protection Act, Section 47 (December 2023), available at https://www.infocom.sc/wp-content/uploads/2024/01/Act-24-2023-Data-Protection-Act-2023.pdf

90 Law 2013-450 on the Protection of Personal Data, Arts. 7 and 26 (June 2013), available at https://www.artci.ci/images/stories/pdf-english/lois_english/loi_2013_450_english.pdf

91 Ordinance No. 15/PR/2018 on Cybersecurity and Cybercrime, Art. 12 (February 2018), available at http://www.droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf

92 Payment Systems (Licensing and Approval) Regulations, Art. 42 (2015), available at https://www.bot.go.tz/Publications/Acts,%20Regulations,%20Circulars,%20Guidelines/Regulations/en/2020030903280842.pdf

### *South Asia (SA) region*[93]

Sri Lanka is the only country in the SA region with its Personal Data Protection Act of 2022,[94] and it will soon be followed by India, which enacted the Digital Personal Data Protection Act in August 2023.[95] The Act will establish a comprehensive data protection framework within the country once it enters into force. India is very active in regulating data transfers, representing an exception in the region. Indian legislation includes localisation policies that affect various types of data, including public sector data, accounting records, and financial data, and restrictions that specifically impact sectors relevant to digital trade, such as cloud computing and telecommunications.

## 5. The recent developments in trade policy discussion on data localisation

The assessment of restrictions on data transfers in trade policy has been subject to intense debate, with some authors claiming that these policies violate trade commitments on services undertaken by members of the World Trade Organisation (WTO).[96] Yet, there is no explicit language on data flows in the WTO.[97] To enhance legal certainty, some countries have incorporated explicit commitments in their preferential trade agreements (PTAs) to refrain from restricting data transfers across borders. In December 2023, there were at least 24 agreements in force with binding language on cross-border data flows and 17 PTAs in force with non-binding language on this issue.[98]

At the same time, there is an ongoing debate at the WTO regarding data policies, both in the General Council with the 1998 Work Programme on Electronic Commerce and among 90 countries with the plurilateral negotiations on a Joint Initiative on E-Commerce (JI). While the 13th WTO Ministerial Conference (MC13) has not seen any meaningful discussion regarding electronic commerce other than continuing the practice of non-imposing duties on electronic transmissions,[99] the co-conveners of the JI have made clear their intent to finalise discussions by mid-2024, stressing the importance of the outcome of these negotiations for the "relevance" of the WTO.[100]

Two recent developments could impact the depth of the commitments on data flows in the JI and, in turn, in future trade agreements. One is the dramatic reversal of the United States' position on data flows announced in October 2023. The country has been the main advocate of binding commitments on data transfers in the past, but it surprisingly withdrew its demands for open cross-border data flows in the JI negotiations, claiming that it needed "policy space" for domestic political discussions on how the government should regulate the activities of tech companies.[101] The second development is the unexpected release of new rules by the Cyberspace Administration of China to soften certain restrictions on data flows[102] driven by economic concerns.[103]

93 The following countries were analysed: Afghanistan, Bangladesh, Bhutan, India, Nepal, Pakistan, and Sri Lanka.

94 Personal Data Protection Act, No. 9 of 2022, Section 26 (March 2022), available at https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf

95 Digital Personal Data Protection Act, 2023 (August 2023), available at https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

96 A. D. Mitchell, and J. Hepburn. "Don't fence me in: reforming trade and investment law to better facilitate cross-border data transfer". 2017. Yale Journal of Law & Technology, Volume 19, p. 182.

97 A. D. Mitchell and N. Mishra, "WTO Law and Cross-Border Data Flows: An Unfinished Agenda" in M. Burri (ed.) Big Data and Global Trade Law. Cambridge: Cambridge University Press, 2021, pp. 83–112.

98 Own calculations based on M. Burri, M. Vásquez, and K. Kugler, "TAPED: Trade Agreement Provisions on Electronic Commerce and Data", available at https://unilu.ch/taped (last accessed in December 2023).

99 World Trade Organization, "Work Programme on Electronic Commerce - Ministerial Decision, WT/L/1193; WT/MIN(24)/38", 2 March 2024, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN24/38.pdf&Open=True (last accessed in March 2024).

100 World Trade Organization, "Co-convenors mark recent round of e-commerce negotiations an important milestone", 14 March 2024, https://www.wto.org/english/news_e/news24_e/ecom_14mar24_e.htm (last accessed in March 2024).

101 Office of the United States Trade Representative, "USTR Statement on WTO E-Commerce Negotiations", 24 October 2023, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations (last accessed in March 2024).

102 Provisions on Promoting and Regulating Cross-Border Data Flows, Cyberspace Administration of China, March 2024, available at https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

103 M. Chorzempa and S. Sacks, "China's new rules on data flows could signal a shift away from security toward growth", *Peterson Institute for International Economics*, 3 October 2023, https://www.piie.com/blogs/realtime-economics/chinas-new-rules-data-flows-could-signal-shift-away-security-toward-growth (last accessed in March 2024).

While it is unlikely that data flows' commitments will be included in the final text of the JI, we might see a renewed ambition to develop interoperable mechanisms to favour data flows across borders, including with countries that have traditionally opposed any commitments on data flows, such as China. These discussions might find more fertile ground in regional fora and set the basis for open plurilateral mechanisms. The main challenge lies in managing the delicate interlinkages between trade, technology and security. Addressing this challenge in the framework of the WTO would signal that this institution can remain relevant in the digital era.

## Annex 1: Data localisation measures in place by 2023

| Country | Law | Policy |
|---|---|---|
| Algeria | Decision No. 48/SP/PC/ARPT/17 dated 29 November 2017 defining the conditions and modalities for establishing and operating of hosting and storage services for computerised content for user benefit in the context of cloud computing services | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** Art. 10 of Decision No. 48/SP/PC/ARPT/17 stipulates that in the course of carrying out the activity covered by its authorisation to establish and operate hosting and storage services for computerised content, the service provider is obliged to establish its infrastructure on national territory and guarantee that it is set up using equipment incorporating the most recent and proven technologies. Furthermore, the service provider is required to provide services via infrastructures specifically declared for this authorisation. The term "service provider" is defined as any natural or legal person who has been granted authorisation to establish and operate hosting and storage services for computerised content for the benefit of remote users as part of cloud computing services, in compliance with the requirements set out in the legislation and regulations in force. |
| Algeria | Decision No. 48/SP/PC/ARPT/17 dated 29 November 2017 defining the conditions and modalities for establishing and operating of hosting and storage services for computerised content for user benefit in the context of cloud computing services | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** Art. 10 of Decision No. 48/SP/PC/ARPT/17 stipulates that in the course of carrying out the activity covered by its authorisation to establish and operate hosting and storage services for computerised content, the service provider is obliged to guarantee that customer data is hosted and stored on national territory and to guarantee a backup solution for data hosted or stored. The term "service provider" is defined as any natural or legal person who has been granted authorisation to establish and operate hosting and storage services for computerised content for the benefit of remote users as part of cloud computing services, in compliance with the requirements set out in the legislation and regulations in force. |
| Algeria | Law No. 18-07 of 25 Ramadhan 1439 corresponding to June 10, 2018 on the protection of natural persons in the processing of personal data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** The last paragraph of Art. 44 of Law No. 18-07 forbids, in any case, the communication or transfer of personal data to a foreign country, when this transfer is likely to carry harm to public security or the vital interests of the state. |
| Algeria | Law No. 18-07 of 25 Ramadhan 1439 corresponding to June 10, 2018 on the protection of natural persons in the processing of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 44 of Law No. 18-07 provides that the data controller may only transfer personal data to another foreign state upon authorisation of the data protection authority and if that state ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing to which such data are or may be subject. Art. 45, however, provides that, by way of derogation to Art. 44, the data controller may transfer personal data to a foreign State subject to certain conditions, including: if the data subject has expressly consented to their transfer; if the transfer is made pursuant to a bilateral or multilateral agreement to which Algeria is a party; with the authorization of the national authority; if the transfer is necessary: (a) to safeguard that person's life; (b) the preservation of the public interest; (c) compliance with obligations to ensure the recognition, exercise or defense of a legal right; (d) the performance of a contract between the controller processing and the data subject, or measures pre-contractual agreements taken at the latter's request; (e) the conclusion or performance of a contract concluded or to conclude, in the interest of the data subject, between the controller and a third party; (f) the execution of a mutual legal assistance measure international; (g) prevention, diagnosis or treatment of medical conditions. |
| Algeria | Decree No. 20-332 Governing the Electronic Press | **Category:** Local processing requirement<br>**Sector:** Media sector<br>**Description:** Art. 6 of Decree No. 20-332 establishes that "the online information activity is subject to the publication through an electronic site, whose hosting is exclusively domiciled, physically and logically in Algeria, with a domain name extension ".dz"." |

| | | |
|---|---|---|
| Algeria | Law No. 18-05 of 24 Chaâbane 1439 corresponding to 10 May 2018 relating to electronic commerce | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** Art. 9 of the Law No. 18-05 requires any e-commerce activity, which is defined as electronic commerce in goods and services, to have a website hosted in Algeria with a ".com.dz" extension. This requirement applies to both domestic and foreign e-suppliers as clarified in Art. 2, which states that states that the legislation applies to e-commerce transactions where one of the parties to the e-commerce contract is: of Algerian nationality, or legally resides in Algeria, or a legal person governed by Algerian law, or if the contract is concluded or performed in Algeria. Effectively, this means that the requirement to have domain names hosted in Algeria also applies to foreign companies. |
| Angola | Law No. 22/11 on the Protection of Personal Data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 24 of the Data Protection Act states that the interconnection of data may only be carried out with the authorisation of the Agência de Protecção de Dados (APD, Data Protection Agency), unless otherwise provided by law. Interconnection of data is defined as a form of processing of personal data consisting of the possibility of linking the data in one file with the data in other file(s) kept by another controller or by the same controller for other purposes. The APD only authorises such interconnection if it is appropriate for the pursuit of the lawful purposes of data processing. As a result, this requirement likely affects cross-border transfers. |
| Angola | Law No. 22/11 on the Protection of Personal Data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Under Section VI of Law No. 22/11, a conditional flow regime is established for the transfer of personal data outside Angola. This means that international data transfer can only proceed if certain conditions are met. The law outlines two main scenarios for international data transfer:<br>- If the country the data is being transferred to can guarantee an adequate level of protection of personal data, then a notification to the Agência de Protecção de Dados (APD, Data Protection Agency) is sufficient to proceed with the transfer, as per Art. 33;<br>- If the country does not provide adequate protection of personal data, then the data controller must obtain authorization from the APD before proceeding with the transfer, as per Art. 34.<br>However, the APD has not issued any decision declaring countries adequate and as a result the authorization remains currently the only means for transfer. |
| Argentina | Law No. 25,326, of October 2000 - Personal Data Protection Law<br><br>Regulation No. 60-E/2016<br><br>Resolution No. 34/2019<br><br>Provision No. 18/2015 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to the Personal Data Protection Law, personal data can be transferred only to countries with an adequate level of protection (Art. 12). These countries, in accordance with Art. 3 of Regulation No. 60-E/2016, include Member States of the European Economic Area (EEA), Switzerland, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada (only in relation to its private sector), Andorra, New Zealand, Uruguay and Israel (only in relation to the data handled automatically). The United Kingdom was included to this list through Art. 1 of Resolution No. 34/2019. In addition, there are exceptions to transfer data abroad, including consent by the data owner, the use of contractual clauses, and binding corporate rules for intra-group international transfer.<br>Provision No. 18/2015, issued by Argentina's National Directorate for Personal Data Protection, treats cloud storage as an international transfer of data, therefore applying the same conditions for the use of these services (Guide to Good Privacy Practices for the Development of Applications, 4.a.7). |
| Australia | My Health Records Act 2012 | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** My Health Records Act 2012 requires information relating to health records to be stored and processed within Australia unless the records do not include "personal information in relation to a healthcare recipient or a participant in the My Health Record System" or "identifying information of an individual or entity" (Section 77). |

| | | |
|---|---|---|
| Australia | Privacy Act 1988 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** In the Privacy Act 1988, the Australian Privacy Principle 8 creates a regime that allows cross-border disclosure of personal information in six different scenarios (Schedule 1). These conditions include but are not limited to situations where there are data protection frameworks that are similar or equivalent to those in Australia, there is consent to the disclosure, or the disclosure is required by laws. The Australian Privacy Principles were inserted into the Privacy Act by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came into force on 12 March 2014. |
| Bahamas | Data Protection (Privacy of Personal Information) Act 2003<br><br>Data Protection Commisioners Guidelines | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 17 of the Data Protection (Privacy of Personal Information) Act 2003 and the Data Protection Commisioners Guidelines, data transfers are permitted where: (i) an adequate level of protection is afforded by a contract; (ii) the transfer is required or authorised by or under any enactment, or required by any convention or other instrument imposing an international obligation on the Bahamas; (iii) the transfer is made pursuant to the consent (express or implied) of the data subject; (iv) the transfer is necessary for the performance of a contract between the data controller and the data subject; among other conditions. |
| Bahrain | Central Bank of Bahrain and Financial Institutions Law of 2006 | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 59 of the Central Bank of Bahrain and Financial Institutions Law of 2006, a licensee must keep accounting records, other records that may be specified by the Central Bank, and separate records for each branch abroad providing any of the services that are subject to the law. Insurance and reinsurance companies must keep records as specified by the Central Bank, including insurance contracts signed by the company, claims made against it and actions taken thereon, reinsurance contracts entered into by the company, and funds to be maintained according to the law (Art. 59). Art. 60 states that the period for which the companies must keep the data is at least ten years and the documents have to be retained at the licensee's main office in Bahrain, or at such other places as the Central Bank may approve. |
| Bahrain | Central Bank of Bahrain Rulebook | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** OM-6.3.1 of Central Bank of Bahrain (CBB) Rulebook provides that conventional bank licensees must maintain the following records in original form or in hard copy at their premises in Bahrain:<br>- Internal policies, procedures and operating manuals;<br>- Corporate records, including minutes of shareholders', directors' and management meetings;<br>- Correspondence with the CBB and records relevant to monitoring compliance with CBB requirements;<br>- Reports prepared by the conventional bank licensee's internal and external auditors; and<br>- Employee training manuals and records.<br>Conventional bank licensees are banks licensed by CBB under Volume 1 of the CBB Rulebook, and generally operating according to conventional finance principals, as opposed to operating in accordance to Islamic finance principles. |

| | | |
|---|---|---|
| Bahrain | Law No. 30 of 2018 with Respect to Personal Data Protection Law<br><br>Order No. 42 of 2022 Regarding the transfer of personal data outside the Kingdom of Bahrain | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 12 of Law No. 30, the transfer of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Alternatively, data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data under several circumstances, including a permission to be issued by the Authority on a case-by-case basis, the consent of the data subject and the necessity to conclude a contract (Art. 13).<br>Order No. 42 establishes a list of countries that have been deemed by the Authority to provide an adequate level of data protection. The adequacy list includes 83 countries, including the UAE, Saudi Arabia, Oman, Jordan, Kuwait, Egypt, India, all EU countries, UK, and USA. Controllers may transfer personal data to any country on the adequacy list without needing to obtain any authorisation from the Authority (Art. 2). |
| Bahrain | Law No. 30 of 2018 with Respect to Personal Data Protection Law<br><br>Order No. 45 of 2022 Regarding the rules and procedures for processing sensitive personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 2 of Order No. 45 provides that sensitive personal data should not be processed without the consent of the data subject, unless one of the cases of Art. 5 of Law No. 30 applies. These include:<br>- The processing is required by the data controllers for their duties and the exercise of their legally prescribed rights in the field of labour relations that binds them to their employees;<br>- The processing is necessary to protect any person if the data subject, their custodian, guardian, or trustee is not legally able to give their consent, and is subject to obtaining prior permission from the Authority;<br>- The processed data was provided by the data subject to the public;<br>- The processing is necessary to initiate or defend any legal rights claim, including what is required in preparation for the matter;<br>- The processing is necessary for the purposes of preventive medicine, medical diagnosis, provisions of health care, treatment, or management of health care services by a licensed medical practitioner or any person legally bound to maintain confidentiality.<br>Controllers also have to implement additional organisational rules when processing sensitive personal data including appropriate high-level technical measures to ensure a high degree of protection against secrecy, breach or unlawful processing of such data (Art. 4 of Order No. 45).<br>Processing is broadly defined in Art. 1 of Law No. 30 and includes disclosing by transmission, dissemination, transference or otherwise making available for others. |
| Bangladesh | Bank Company Act, 1991 - Act No. 14 of 1991 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Section 12 of the Bank Company Act provides that banks may not transfer records or documents relating to its business outside Bangladesh unless such transfer is given prior approval by the Central Bank. This restriction is specific to banks only. |
| Barbados | International Trusts Act 1995 | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** Under Section 13.1.b of the International Trusts Act 1995, a trustee of an international trust created under Section 10 shall keep in Barbados a register in which the following information is set out: the name of the settlor, a summary of the purposes of the trust, the name of the protector of the trust, and such documents as are necessary to show the true financial position of the trust. |

| | | |
|---|---|---|
| Barbados | Companies Act 1982 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Section 170 of the Companies Act 1982 lists a series of registers and records that must be maintained at a company's registered office or at some other place in Barbados designated by the directors of the company, including minutes of meetings and resolutions of shareholders, the name and latest known address of shareholders, and a register showing the name and latest known address of each person to whom privileges, options or rights have been granted. In addition, under Section 172 of the Companies Act, adequate accounting records and records containing minutes of meetings and resolutions of the directors and any committees of the directors shall be kept at the registered office of the company or at some other place in Barbados designated by the directors. Furthermore, according to Section 172.3, when any accounting records of a company are kept at a place outside Barbados, accounting records that are adequate to enable the directors to ascertain the financial position of the company with reasonable accuracy on a quarterly basis must be kept at the company's registered office or at some other place in Barbados designated by the directors. |
| Barbados | Income Tax Act 1969 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Under Section 75.1 of the Income Tax Act 1969, every person carrying on business and every person who is or may be required by the Act to collect or pay a tax or other amount shall keep records and books of account, including an annual inventory, in Barbados, in such form and containing such information as will enable the taxes payable under the Act or the taxes or other amounts that should have been deducted, withheld or collected to be determined. |
| Barbados | Data Protection Act 2019 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 22 of the Data Protection Act 2019, personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for: (i) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and (ii) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects. |
| Belgium | VAT Code of 1969 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** All incoming and outgoing invoices must be stored on Belgian territory for seven years. However, invoices which are stored electronically and which guarantee full online access to the data concerned in Belgium may be stored in another Member State of the European Union on condition that the fiscal administration is informed of this in advance (Art. 60 of the VAT Code). Moreover, taxpayers who are not established in Belgium must provide a Belgian address to the authorities where books, (copies of) invoices and other documents can be provided upon the request of the authorities (Art. 61, § 1 of the VAT Code). This also applies to digital documents. |
| Belgium | Income Tax Code of 1992 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Arts. 315 and 315 *bis* of the Income Tax Code require that the books and records necessary to determine the amount of taxable income must be kept by companies for seven years following the taxable period. The documentation must be kept in the professional or private premises of the taxpayer where the administration can carry out the necessary inspection. |
| Benin | Law No. 2009-09 of 22 May 2009 Dealing with the Protection of Personally Identifiable Information | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Section 43 of Law No. 2009-09 provides that transfer of personal data to another country or an international organization requires prior authorization from the Regulator. |

| | | |
|---|---|---|
| Benin | Law No. 2017-20 of 20 April 2018 on the Digital Code in the Republic of Benin | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 391 of Law No. 2017-20 requires that the transfer of personal data to a third State or international organisation may only take place when the Authority finds that the State or international organisation in question ensures a level of protection equivalent to that provided for in the law. Art. 392 provides some exceptions, including the express consent of the data subject and the necessity of the transfer for the execution of the contract. |
| Botswana | Companies Act, 2007 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to Sections 189 and 190 of the Companies Act, 2007, a company limited by shares must keep accounting records including invoices relating to the sale and supply of goods at its registered office or such other place in Botswana as the board of the company shall determine. |
| Botswana | Data Protection Act, 2018 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 20 of the Data Protection Act (DPA) prohibits processing of sensitive personal data except under certain circumstances. These include:<br>- The processing is specifically provided for under the DPA;<br>- The data subject has given consent in writing;<br>- The data subject has made the data public;<br>- The processing is necessary for national security, for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, or where the processing is authorized by any other written law for any reason of substantial interest to the public; or<br>- The processing is necessary to protect the vital interest of a data subject and another person in a case where consent cannot be given by or on behalf of the data subject, the data controller cannot be reasonably expected to obtain consent or the consent by or on behalf of the data subject has been unreasonably withheld.<br>It is not clear whether a data transfer is considered a form of processing. |
| Botswana | Data Protection Act, 2018 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 48 of the Data Protection Act (DPA) prohibits the transfer of personal data from Botswana to another country, unless the personal data is transferred to a third country that ensures an adequate level of protection. Such level of protection will be assessed by the Commissioner in light of all the circumstances surrounding the data transfer operation in accordance with Sections 49 (1)-(4). Alternatively, the transfer is allowed if there is the consent of the data subject or where the transfer is:<br>- Necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre contractual measures taken in response to the data subject's request;<br>- Necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party;<br>- Necessary for the public interest, or for the establishment, exercise or defence of a legal claim;<br>- Necessary to protect the vital interests of the data subject; or<br>- Made from a register that is intended to provide the public with information and is open to public inspection. |

| | | |
|---|---|---|
| Brazil | Normative Instruction of the Secretariat of Management No. 1 - Public Procurement of Cloud Computing Services Guidelines<br><br>Complementary Regulations No. 14/IN01/DSIC/SCS/GSIPR | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** Section 4 of the Annex of Normative Instruction on Public Procurement of Cloud Computing Services requires the existence of a national data centre. However, only classified information (reserved, secret and ultra secret) must be stored in the country. This results from the regulations of the Institutional Security Cabinet, especially Complementary Regulations No. 14/IN01/DSIC/SCS/GSIPR, which state that classified information should be exclusively stored in Brazil. The model terms of reference for procurement clarify this requirement. On the other hand, it is up to the high management of the public organization to define which information can be stored in the national territory or abroad. |
| Brazil | Resolution CMN No. 4.893<br><br>Resolution BCB No. 85 | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Art. 12 of Resolution CMN No. 4.893 and Art. 12 of Resolution BCB No. 85 state that institutions authorised to operate by the Central Bank of Brazil (Banco Central do Brasil, BCB) may contract cloud and data processing services in Brazil or abroad as long as they adopt corporate governance practices proportionate to the service hired and the risks to which they are exposed to; and verify the capability of the potential service to ensure compliance with the current legislation, institution's access to data, the confidentiality and integrity of data, adherence to certification patterns required by the institution, access to auditing reports, provision of information and management resources appropriate to the monitoring of services provided, identification of the institution's customer data and quality of access controls aimed at protecting customer's data. In addition, Art. 15 of both Resolutions establishes that the companies should notify to BCB the countries where financial data is processed. Also, Art. 16 of both Resolutions provides that the contracting of data processing, data storage and cloud computing relevant services provided abroad must fulfil the following requisites:<br>- The existence of an agreement for exchange of information between the BCB and the supervisory authorities of the countries where the services may be provided;<br>- The contracting institution must ensure that the provision of the services do not cause damage to its own functioning neither do they deter the action of the BCB;<br>- The contracting institution must define, previously to the contracting, the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed;<br>- The contracting institution must anticipate alternatives for business continuity either in the case of impossibility of continuation of the contract or in the case of its termination.<br>The BCB's prior approval must be obtained if the institutions retains a cloud service provider in countries where there is no agreement to exchange information between the BCB and the competent authorities. The institutions must request such approval from the BCB at least 60 days before retaining the cloud services in question. |
| Brazil | Law No. 13.709 of 14 August 2018, General Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The Personal Data Protection Law allows the international transfer of personal data only under certain conditions (Arts. 33-36). The main conditions for such a transfer are that the recipient jurisdiction has an adequate level of data protection; the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); the data subject has given his/her consent explicitly; or the transfer is necessary for the performance of a contract between the data subject and the controller. Art. 11 provides stricter conditions for processing of sensitive personal data and it is reported that in practice these conditions forced many organizations to store privacy-sensitive data in Brazil. The law applies extraterritorially to all companies that target Brazilian consumers even when the company is not established in the Brazilian market. |

| | | |
|---|---|---|
| Brunei | Data Protection Policy, 2014 | **Category:** Conditional flow regime<br>**Sector:** Public sector<br>**Description:** The Data Protection Policy (DPP) 2014 applies only to public agencies, including government Ministries and Departments, educational institutions and statutory bodies. The Law (Section 18) provides that the agencies are only permitted to transfer personal data to a party outside of Brunei if:<br>- There is a reasonable belief that the recipient is subject to a law, binding scheme or contract, which upholds principles for fair data handling substantially similar to the DPP;<br>- The individual has provided consent;<br>- It is necessary for contract performance or pre-contractual obligations;<br>- Reasonable steps have been taken to ensure the data will not be used, held or disclosed by the recipient inconsistent to the DPP.<br>This policy applies to all data including personal data already in existence whether or not by electronic means (Section 4.4). |
| Bulgaria | Gambling Act | **Category:** Local processing requirement<br>**Sector:** Gambling sector<br>**Description:** According to Art. 6 of the the Gambling Act, when applying for a gaming license all relevant data must be stored on a server in Bulgaria. Communications equipment and the central computer must be located in the European Economic Area (EEA) or Switzerland. |
| Burkina Faso | Law No. 001-2021/AN protecting people with regard to the processing of personal data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** According to the Art. 37 of Law No. 001-2021/AN, health data allowing the direct or indirect identification of individuals must be stored on national territory. An exception can be granted if the Commission For Information Technology and Civil Liberties (Commission de l'Informatique et des Libertés, CIL) ensures that the use of information and communication technologies for the purpose of processing personal data does not pose a threat to individual or public freedoms and privacy (Art. 56). |
| Burkina Faso | Law No. 001-2021/AN protecting people with regard to the processing of personal data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** According to the Art. 42 of Law No. 001-2021/AN, international transfers cannot be made without the respect of the following conditions:<br>- a request of authorisation of the Commission for Information Technology and Civil Liberties (Commission de l'Informatique et des Libertés, CIL));<br>- a signature of a data confidentiality clause and a data reversibility clause in order to facilitate the complete migration of the data at the end of the contract;<br>- the implementation of technical and organisational security measures.<br>Additionally, the transfer can only be made to a foreign country or an international organisation if the recipient country or international organisation ensures an adequate level of protection equal to the one ensured in Burkina Faso. |
| Cabo verde | Law No. 133/V/2001, of 22 January: establishes the general legal regime for the protection of personal data of natural persons | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 19 of Law No. 133/V/2001 provides that transfer of personal data outside of Cabo Verde is only permissible if the foreign country ensures an adequate level of protection. However, according to Art. 20, the transfer of personal data to a country which does not ensure an adequate level of protection may be permitted by Comissão Nacional de Proteção de Dados Pessoais (CNPD, National Commission of Data Protection) if the data subject has given consent to the transfer or under limited exemptions provided for by the law. |

| | | |
|---|---|---|
| Chad | Law No. 007/PR/2015 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Processing of special categories of data (including sensitive data) is prohibited unless consent of the data subject is obtained (Chapter V of Law No. 007/PR/2015 on the protection of personal data). According to Art. 52, authorization of the "Agence Nationale de Sécurité Informatique et de Certification Électronique" (ANSICE), is mandated to process this data. It is not clear how this requirement affects the capacity of companies to transfer data across borders.<br>Art. 29 of Law further prohibits the transfer of personal data to a country that is not a member of the Economic and Monetary Community of Central Africa (CEMAC) or the Economic Community of Central African States (ECCAS), unless that state ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. Certain exceptions apply (Art. 30-33). Prior to any transfer of personal data abroad, it is required that the data controller informs the regulatory authority, the National Agency for Information Security and Electronic Certification (ANSICE). |
| Chile | Updated Compendium of Banking Regulations - Chapter 20-7 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Section IV.1.b.i of Chapter 20-7 of the Updated Compendium of Banking Regulations requires operators outsourcing data processing services outside the country to have a contingency data processing centre located in Chile. It is reported that this would not be very different from requiring the main centre to also be local. This requirement is for institutions that carry out activities abroad that are considered significant or strategic and they must demonstrate a recovery time compatible with the criticality of the outsourced service. |
| China | Data Security Law of the People's Republic of China | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 31 of the Data Security Law provides that the security administration of the cross-border transfer of important data collected and generated by critical information infrastructure operators during their operation in China shall be subject to the provisions of the Cybersecurity Law of the People's Republic of China; the administrative measures for the cross-border transfer of important data collected and generated by other data processors during their operation in China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council. In addition, Art. 36 stipulates that the competent authority of China shall process the request for providing any data from a foreign judicial body and law enforcement body in accordance with relevant laws and the international treaty or agreement which China has concluded or acceded to, or under the principle of equality and mutual benefit. Any organisation or individual within the territory of China shall not provide any foreign judicial body and law enforcement body with any data stored within the territory of the People's Republic of China without the approval of the competent authority of China. |
| China | Yinfa No. 17 [2011], Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions<br><br>Personal Financial Information Protection Technical Specification | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** The "Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions" states that the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China and such personal information is not allowed to be transferred overseas (paragraph 6).<br>The Personal Financial Information Protection Technical Specification (PFI Specification) regulates “any personal information collected, processed and stored by Financial Institutions during the provision of financial products and services" (PFI). The PFI specification requires that PFI collected or generated in mainland China is stored, processed and analysed within the territory. Further, under the PFI Specification, where there is a business need for cross-border transfer of personal financial information (PFI) and the financial institution obtains explicit consent to the transfer from the personal financial information subjects (i.e the persons under the PFI Specification providing the data), conducts a security assessment and then supervises the offshore recipient to ensure responsible processing, storage and deletion of PFI (Section 7.1.3). |

| | | |
|---|---|---|
| China | Administrative Measures for Population Health Information (For Trial Implementation) | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas (Art. 10). |
| China | Amendment to the Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The 2020 Specification provides that where personal biometric information must not be shared or transferred unless actually essential for business needs in which case the personal information subject must be separately informed of the purpose, types of biometrics involved, identification of the recipient and its data security capacity and the personal information subject consent must be explicitly obtained (9.2.i). |
| China | Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Article 5.4.5 of the Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems prohibit the transfer of personal data abroad without express consent of the data subject, government permission or explicit regulatory approval "absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities". If these conditions are not fulfilled, "the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas."<br><br>Although the Guidelines are a voluntary technical document, they might serve as a regulatory basis for judicial authorities and lawmakers. |
| China | Personal Information Protection Law | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** The Personal Information Protection Law (Art. 40) provides that critical information infrastructure operators and personal information processors handling personal information must store personal information collected and produced within the borders of China. Where such information needs to be provided abroad, they shall pass a security assessment organized by the national cyberspace department. Also, according to Art. 38, the processors of personal information must apply one of the conditions to provide information outside of PRC: passing the security assessment organized by the national cyberspace department in accordance with Art. 40 of this Law; obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department; concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.<br>Where a processor of personal information provides personal information outside the People's Republic of China, it is required to inform the individual of the name or names of the overseas recipient, the contact information, the purpose of processing, the manner of processing, the type of personal information, as well as the manner and procedure for the individual to exercise his or her rights under this Law with the overseas recipient, and obtain the individual's individual consent (Art. 39). Personal information processors shall not provide personal information stored in the People's Republic of China to foreign judicial or law enforcement agencies without the approval of the competent authorities of the People's Republic of China (Art. 41). |

| | | |
|---|---|---|
| China | Cybersecurity Law<br><br>Outbound Data Transfer Security Assessment Measures | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 37 of the Cybersecurity Law requires "key information infrastructure" operators to store personal information and critical data within China. Personal information and critical data can be stored outside of China where there is a genuine need for business; in such case a "security assessment" needs to be conducted in accordance with procedures formulated by the Cyberspace Administration of China (CAC) in collaboration with other authorities.<br>Art. 4 of the Outbound Data Transfer Security Assessment Measures, promulgated by the CAC, outlines four situations where a security assessment is necessary before an outbound transfer can take place: 1) In cases where the transfer concerns “important data”, which is broadly defined as data that could endanger national security, economic operation, social stability, public health and safety; 2) In case the transfer concerns personal data by a critical information infrastructure operator or processor of personal information that processed data for 1 million or more individuals; 3) Also in the case of transfers concerning personal data by a personal information processor that has made outbound transfers of personal information of 100,000 individuals or sensitive personal information of 10,000 persons in the preceding year; 4) Lastly, the CAC may also require security assessment in other situations which are not further defined.<br>Art. 8 of the Measures covers the factors that the CAC will take into account when undertaking a security assessment. The assessment includes a wide range of aspects, for example:<br>- The risks that the transfer may entail for national security or public interests, among other policy objectives;<br>- Legitimacy, necessity and method of transfer;<br>- Whether the level of data protection in the recipient country meets the requirements of laws in China;<br>- Sensitivity of the data and risks of being tampered with abroad;<br>- Agreed safeguard measures between the data processor and data recipient;<br>- Any other matter that the CAC deems necessary.<br>In case of unfavourable outcomes, the data handler can ask the CAC for a re-assessment with a final decision. In case of a positive decision, the permission to transfer data abroad is valid for two years but if substantial changes in the risk factors arise, a new assessment might be needed. |
| China | Map Management Regulations | **Category:** Local processing requirement<br>**Sector:** Maps sector<br>**Description:** Online maps are required to set up their server inside of the country (Art. 34 of Map Management Regulations) and must acquire an official certificate. |
| China | Interim Measures for the Administration of Online Taxi Booking Business Operations and Services | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** China instituted a licensing system for online taxi companies which requires that the personal information and business data should be stored and used in mainland China and must not be transferred outside of China (Art. 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services). Such information should be retained for two years, except when otherwise required by other laws and regulations. The Measurement also regulates that servers of the taxi companies should be set up in Mainland China, with a network security management system and technical measures for security protection in compliance with regulations (Art. 5.2). |
| China | Telecommunications Regulations of the People's Republic of China | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** China's Telecommunications Regulations require all data collected inside China to be stored on Chinese servers. It is reported that as a result of this regulation, Hewlett Packard, Qualcomm, and Uber were required to divest more than 50% of their businesses in China to Chinese companies, to avoid fines. |

| | | |
|---|---|---|
| China | Provisional Measures for Administration of Business Activities of Internet Lending Information Intermediaries | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 27 of the Provisional Measures for Administration of Business Activities of Internet Lending Information Intermediaries, the lender and borrower information collected within China shall be stored, processed, and analyzed in China. Unless otherwise provided by laws and regulations, online lending information intermediaries shall not provide information of domestic lenders and borrowers to overseas. |
| China | Regulation on the Administration of Credit Investigation Industry | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 24 of the Regulation on the Administration of Credit Investigation Industry, organizing, preserving and processing of consumer or commercial data by credit reporting agencies must take place within China. |
| Colombia | Law No. 1,266 Regulates habeas data and the handling of the information contained in personal databases, especially financial, credit, commercial, services and that from third countries […] | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Art. 5 of Law No. 1,266 establishes a rule on international data transfers as carried out by data bank operators. The transfer is permitted to other data operators when there is authorization from the data subject; or when the destination database has the same purpose as the operator that delivers the data.<br><br>If the receiver of the data is a foreign data bank, the delivery without authorization must be done with a written record and due verification by the operator that the laws of the recipient of the information offer guarantees for the protection of the rights of the data subject. |
| Colombia | Law No. 1,581 Data Protection Law<br><br>Decree No. 1,377 Which Partially Regulates Law No. 1,581 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 26 of Law No. 1,581, cross-border transfer of personal data is forbidden unless it is made to a country that offers adequate levels of data protection (as defined by the Colombian data protection authority). The above-mentioned prohibition does not apply in certain cases, including when the data subject authorizes the cross-border transfer, or in the case of medical data being required for health or public hygiene reasons. According to the law, the institution in charge, "Superintendencia de Industria y Comercio" (SIC), establishes the standards regarding international data transfers. |
| Congo | Law 29-2019 on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Law No. 29-2019 states that the transfer of data abroad is possible if:<br>- the third country ensures a sufficient level of protection of privacy, fundamental rights and freedoms of people (Art. 23),<br>- the person to whom the data relates has agreed to their transfer;<br>- the transfer is necessary to protect that person's life, to safeguard the public interest and the execution of the contract between the interested party and the data manager (Art. 24). |
| Costa Rica | Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 31(f) of Law No. 8968, transferring personal information of Costa Ricans or resident foreigners in the country to databases located in third countries without the consent of its owners is considered a very serious offense. |
| Cote d'Ivoire | Law No. 2013-450 of June 19, 2013 relating to the protection of personal data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Under Art. 26 of Law No. 2013-450, the controller of a processing operation may only be authorized to transfer personal data to a third country if that country ensures a higher or equivalent level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing of which such data are or may be subject. In addition, before any actual transfer of personal data to this third country, the controller must first obtain authorization from the Protection Authority. The transfer of personal data to third countries is subject to regular monitoring by the Protection Authority with regard to their purpose. |

| | | |
|---|---|---|
| Cuba | Decree No. 360/2019 On the Security of Information and Communication Technologies and the Defense of National Cyberspace<br><br>Decree Law No. 370/2019 On the Informatization of Society in Cuba | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 68(f) of Decree Law No. 370 states that the use of foreign servers to host websites is an offence. According to Art. 82 of Decree No. 360/2019, "when due to connectivity needs or other interests, the entity requires hosting a site on servers located in a foreign country, this is done as a mirror or replica of the main site on servers located in Cuba and the required measures are established to guarantee their security, in particular during the process of updating the information. In addition, according to Art. 83, "The network servers of an entity intended to facilitate access to or from abroad and those for internal use must be installed in different areas of the network, in such a way as to avoid connection between them." |
| Cuba | Law 149/2022 on Personal Data Protection | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Law 149/2022 includes provisions for cross-border data transfer and outlines that there are only five specific exceptions for data transfers outside the country. The cross-border data transfer is therefore only allowed in the case of international judicial cooperation, exchange of medical data when necessary for the treatment of the data subject, bank or stock exchange transfers about the relevant transactions, under applicable international treaties, and if the transfer of data is for the purpose of international cooperation in the fight against crime (Art. 65.1). In addition, Art. 66 grants to certain authorities the competencies to authorise the international transfer of personal data in other circumstances. |
| Denmark | Act No. 502 of 23 May 2018 on Supplementary Provisions to the Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Data Protection Act)<br><br>Danish Executive Order No. 1104 of 30 June 2020 | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Section 3(9) of the Danish Data Protection Act mandates the Minister of Justice to lay down rules requiring that personal data processed in specific IT systems, which are held for the public administration, must be kept in whole or in part in Denmark. In 2020, the Danish Minister of Justice issued Danish Executive Order No. 1104 of 30 June 2020, which states that the following IT systems shall be maintained in Denmark:<br>- DeMars: the Defence Management and Resource Control System;<br>- Digital Post: the system to digitally provide all post from Danish authorities to citizens;<br>- MitID: Denmark's digital ID;<br>- NemLog-in3: online public self-service solutions;<br>- Statens Lønløsning: the systems to manage salary and pension payments to all government employees. |
| Dominican Republic | Personal Data Protection Law No. 172-13 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 80 of the Law No. 172-13, personal data may only be transferred internationally if the owner of the data expressly authorizes such transfer, or if such transfer is necessary for the performance of a contract between the owner of the data and the person or entity responsible for the treatment of the personal data. Data transfer is considered a form of 'treatment' of personal data under Art. 6.20 of Law. |
| DRC | Law No. 20/017 on telecommunications and information and communication technologies | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 132 of Law No. 20/017 provides that the collection, recording, processing, storage and transmission of personal data shall be carried out with the authorisation of the user concerned or of the competent public authority. The definition of processing in Art. 4 encompasses the transfer of data. Moreover, it is prohibited the collection and processing of personal data revealing the racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data or more generally data relating to the state of health of the person concerned.<br>Art. 2 states that Law No. 20/017 applies to the various activities of the telecommunications and information and communication technologies sector on national territory and it also applies to any processing of personal data by a natural person or legal entity under public or private law, and by the public sector. |

| | | |
|---|---|---|
| Ecuador | Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 56 of the Personal Data Protection Law, personal data can be transferred to countries that comply with internationally recognized standards in accordance with the criteria that will be established in the regulation of the law, which are not yet published. When necessary due to the nature of the transfer, the Personal Data Protection Authority may implement ex-post control methods. According to Art. 60 of the law, without prejudice to the provisions of the preceding articles, international transfers or communications of personal data may be carried out in some circumstances including with the explicit consent of the data subject, for the fulfillment of institutional competencies, to comply with a legal or regulatory obligation, and for the performance of a contract between the holder and the controller of the personal data. |
| Ecuador | Organic Code on the Social Economy of Knowledge, Creativity and Innovation<br><br>Law for the Development of Technological Financial Services, Fintech Law | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Art. 146 of the Organic Code on the Social Economy of Knowledge, Creativity and Innovation stipulates that when public sector entities contract technological services to third parties, they must ensure that information or data that has been classified as reserved and confidential for reasons of national security and that belongs to the Ecuadorian state must be stored in data centres or computer platforms located in Ecuadorian territory. Prior to its amendment by the Fintech Law in 2022, the Code stipulated that data pertaining to national security and strategic sectors had to be stored in computer centres located within Ecuadorian territory. Furthermore, data of relevance to the State had to be stored in computer centres located within Ecuadorian territory or in countries with data protection standards that are at least as stringent as those established in Ecuador. |
| Egypt | Resolution No. 151 of 2020 approving the Law on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 14 of Law No. 151 of 2020 on Personal Data Protection prohibits the transfer of personal data to a foreign country unless the laws of the foreign country guarantee a minimum level of protection that is equal to the level stipulated by Egyptian law. Moreover, the transfer of data abroad requires an authorisation or a license from the Data Protection Centre. Art. 15 enumerates several specific exceptions to the obligation of Art. 14 subject to the express consent of the person concerned with the data or his representative. |
| Egypt | Law No. 180 of 2018 Regulating the Press, Media, and the Supreme Council for Media Regulation<br><br>Cabinet Resolution No. 418 of 2020 | **Category:** Local storage requirement<br>**Sector:** Media sector<br>**Description:** Art. 16 of the Executive regulation (Cabinet Resolution No. 418 of 2020) relating to Law No. 180 of 2018 Regulating the Press, Media, and the Supreme Council for Media Regulation (SCMR) requires media outlets and websites to have a backup of their electronic servers within the Arab Republic of Egypt, provided that it is safe and known to the SCMR. The term “media” is defined as “any terrestrial or satellite television channel, or wired, wireless or electronic radio station”. |
| Egypt | Law No. 180 of 2018 Regulating the Press, Media, and the Supreme Council for Media Regulation<br><br>Cabinet Resolution No. 418 of 2020 | **Category:** Local storage requirement<br>**Sector:** Media sector<br>**Description:** Art. 35 of Egypt's Media Law No. 180 of 2018, and Arts. 5 and 16 of its executive regulation (Cabinet Resolution No. 418 of 2020) stipulate that newspapers must be printed in presses inside the Arab Republic of Egypt and a backup of the electronic servers hosting their electronic copies must be located in a place specified by the newspaper within the Arab Republic of Egypt, provided that it is safe and known to the Supreme Council for Media Regulation (SCMR). |

| | | |
|---|---|---|
| Egypt | Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation<br><br>Resolution of the Council of Ministers No. 418 of 2020 Issuing Executive Regulations for Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation | **Category:** Local processing requirement<br>**Sector:** Media sector<br>**Description:** According to Art. 16 of the Resolution of the Council of Ministers No. 418 of 2020 Issuing Executive Regulations for Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation, all companies having a licence from the Supreme Council for Media Regulation (SCoM) to operate and distribute recorded or live content in Egypt, whether through satellite or the internet, are required to store all content for at least one year in a server that is located at a secure location in Egypt. The location may not be changed without prior approval from the SCoM. |
| El Salvador | Law for the Regulation of Information Services on Credit History of Persons | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 17 of the Law for the Regulation of Information Services on Credit History of Persons, as amended in September 2021, establishes that legal persons operating as data information agencies have the duty to maintain the database and its backup in the country. A data information agency is defined in Art. 3 as any legal person, public or private, with the exception of the "Superintendencia del Sistema Financiero" (Financial System Superintendency), which is engaged in collecting, storing, preserving, organising, communicating, transferring or transmitting data on the credit history of consumers or clients, through technical procedures, automated or not. |
| Equatorial Guinea | Law No. 1/2016 on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Arts. 27 and 28 of Law No. 1/2016 provide that organizations may not transfer any personal information to countries that fail to provide a legally equivalent level of protection, unless the transfer has been previously authorized by the Governing Body for the Protection of Personal Data or under some exceptions, such as consent or contractual necessity. It is reported that the Governing Body for the Protection of Personal Data has not yet been established and there is no list of legally equivalent countries. |
| Eswatini | Data Protection Act, 2022 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 32(1) of the Data Protection Act provides that if a Southern African Development Community (SADC) Member State has transposed the requirements under the SADC Model Law on Data Protection, the transfer of data is permitted. SADC is an economic block covering 16 countries in Southern Africa. Moreover, the transfer is permitted where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of the data controller, or where the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State (Sections 32(1)(a) and (b)).<br>In addition, Section 33 of the Act permits the transfer of personal information to other recipients if an adequate level of protection is ensured in the country and the data is transferred solely to permit processing authorised by the controller. Apart from the above requirements, transfers of personal data are permitted where the data subject has unambiguously given their consent to the proposed transfer, the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken in response to the request of the data subject, among others (Sections 33(4)(a-f)). |
| Ethiopia | Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art 12.7 of Directive No. ONPS/02/2020, point of sale machine operators are not allowed to send domestic payment information outside Ethiopia for the purpose of authorisation, clearing and settlement. They can only send payment data made through the international card scheme to the financial institution or national switch. Similarly, automated teller machine operators cannot send any transaction outside Ethiopia for the purpose of processing, authorisation and switching (Art. 11.1). |

| | | |
|---|---|---|
| EU | General Data Protection Regulation (Regulation 2016/679) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The EU's General Data Protection Regulation (GDPR) considerably expands the scope of EU privacy rules. In addition to companies established in the EU, the Regulation applies extraterritorially to companies offering goods or services to data subjects in the EU and companies that monitor the behavior of EU citizens (Art. 3).<br>The Regulation mandates that data is allowed to flow freely outside the European Economic Area (EEA) only in certain circumstances listed in Chapter 5 of the Regulation. The main conditions for such a transfer are the following: the recipient jurisdiction has an adequate level of data protection; the controller ensures adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); the data subject has given his/her consent explicitly; or, the transfer is necessary for the performance of a contract between the data subject and the controller.<br>The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection. In addition, the EU-US Data Privacy Framework acts as a self-certification system open to certain US companies for data protection compliance since July 2023. |
| Finland | Accounting Act 1336/1997 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** The Accounting Act (Chapter 2, Sections 7 and 9) requires that a copy of the accounting records be kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed. |
| France | Tax Procedures Handbook | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to the Art. L102 C of the Tax Procedures Handbook, if invoices are sent in electronic form, taxable persons may not store invoices in a country not linked to France by an agreement providing for mutual assistance or not providing immediate online access rights, downloading and use of the whole of the data concerned. Taxable persons are obliged to declare the place of storage of their invoices and any modification of that place where it is located outside France. |
| France | Heritage Code | **Category:** Local storage requirement<br>**Sector:** Public sector<br>**Description:** Under Arts. L-111-1 and L-111-2 of the Heritage Code, public archives that are kept because of scientific interest or ongoing administrative utility are national treasures. As such, they must be stored on French territory, even in electronic form. |

| | | |
|---|---|---|
| Gabon | Law No. 001/2011 of September 25, 2011 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 94 of the Data Protection Law, the transfer of personal data to another country is prohibited unless the destination country ensures an adequate level of privacy protection, and protection of fundamental rights and freedoms of individuals with regard to the processing operation. Determination of adequacy is a prerogative of the Gabon Data Protection Authority (the Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP)), taking into consideration the following factors:<br>-the legal provisions existing in the country in question;<br>-the security measures enforced;<br>-the specific circumstances of the processing (such as the purpose and duration thereof); and<br>-the nature, origin, and destination of the data.<br>As an alternative to the 'adequacy' criteria, data controllers may transfer data if the data subject has consented expressly to its transfer; the transfer is necessary to save that person's life; the transfer is necessary to safeguard a public interest; the transfer is necessary to ensure the right of defence in a court of law; or the transfer is necessary for the performance of a contract between the data subject and the data controller, at the request of the data subject, or for the performance of a contract between the data controller and a third party in the interest of the data subject (Art. 95). |
| Gabon | Law No. 001/2011 of September 25, 2011 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 47 of Chapter IV of the Data Protection Law prohibits collecting or processing sensitive data (that is, data which reveal racial or ethnic origins, political, philosophical, or religious opinions or trade union membership of data subjects, or which relate to their health or sex life) barring certain exceptions, such as under explicit consent of the data subject as guided by the law, and when it serves the purposes of preservation of life. |
| Gabon | Ordinance No. 00000015 / PR / 2018 of 23 February 2018 regulating cybersecurity and the fight against cybercrime in the Gabonese Republic | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 12 of the Ordinance Regulating Cybersecurity and the Fight Against Cybercrime requires electronic communications network operators to have an operational management center for their infrastructures in the national territory. |
| Gabon | Ordinance No. 00000015 / PR / 2018 of 23 February 2018 regulating cybersecurity and the fight against cybercrime in the Gabonese Republic | **Category:** Local storage requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 19 of the Ordinance Regulating Cybersecurity and the Fight Against Cybercrime mandates electronic communication network operators and information systems operators to host a copy of their connection and traffic data, in the national territory. |
| Gambia | The Gambia Draft Data Protection and Privacy Policy 2019 | **Category:** Conditional flow regime<br>**Sector**: Horizontal<br>**Description:** Section 9 of the Gambia Draft Data Protection and Privacy Policy 2019 allows for cross-border transfer of personal data only where an appropriate level of protection is guaranteed. This is the case when:<br>- An assessment by the Gambian data controller that the receiving country has protective measures for data received under international agreements or approved standardised and binding safeguards;<br>- A data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards ensuring data protection;<br>- Legitimate interests such as public interests.<br>However, being a guideline, this policy has no force of law and therefore is not legally binding. |

| | | |
|---|---|---|
| Germany | Digital Health Appliances Ordinance | **Category:** Conditional flow regime<br>**Sector:** Health sector<br>**Description:** Under the Digital Health Appliances Ordinance, data related to digital health appliances, can only be processed in the EU or in jurisdictions where there is an adequacy decision (Section 4(3)), while other exceptions such as standard contractual clauses are not allowed. Digital Health Appliances (Digitale Gesundheitsanwendungen) are low risk, medical digital devices that are intended to detect or alleviate illnesses, that assist in diagnosis, and that are based primarily on digital technology. They include apps, or browser-based applications. A "DiGA" can be used either by the patient alone or shared by the doctor and patient. |
| Germany | The Fiscal Code of Germany | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Pursuant to Section 146 of the Fiscal Code, financial accounts and records must be kept within Germany. Exceptionally, the competent revenue authority may authorise the storage of electronic accounts data outside of Germany if certain conditions are met (e.g., information is given about the location of the data processing and name of the third party processor; the data remains fully accessible and taxation is not hampered). |
| Germany | Value Added Tax Act | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to §14b of the Value Added Tax Act, all VAT invoices must be stored within Germany. When these invoices are stored electronically, they can be stored within another EU member state. However, the tax authority must be notified of the location of the data servers, and have the ability to access and download the data. |
| Ghana | Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930)<br><br>Banking Act 2004 (Act 673) | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** Section 79(3) of Act 930 provides that the accounting records of the bank, specialised deposit-taking institution or financial holding company shall be kept at the head office in the country for a period of not less than ten years. Previously, Section 71(2) of Act 673, which was repealed by Act 930, also required a bank to keep its accounting records at the bank's head office in Ghana. |
| Greece | Law 4002/2011 Amendment of the state pension legislation - Arrangements for growth and fiscal consolidation - Issues of responsibility of the Ministries of Finance, Culture and Tourism and Labor and Social Security | **Category:** Local storage requirement<br>**Sector:** Gambling sector<br>**Description:** Art. 47 of Law 4002/2011 requires that data relating to the conduct of online gambling, as well as data exchanged between a player, licensee, internet service provider and financial institutions relating to such games are stored in servers located in Greece for a period of 10 years. |
| Greece | Data Retention Directive 2006/24/EC<br><br>Judgment European Court of Justice in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others<br><br>Law 3917/2011 Data retention produced or subjected to processing in relation to the provision of services of electronic communications available to the public or public communication networks, use of systems of surveillance with the storing or reception of sound or image in public spaces and related provisions | **Category:** Local storage requirement<br>**Sector:** Telecom sector<br>**Description:** Under the EU Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid. However, not all national laws which implemented the Directive have been overturned. The Greek law implementing the Directive is still in place. Art. 6 of Law 3917/2011 goes even further in the implementation of the Data Retention Directive by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory.' |

| | | |
|---|---|---|
| Guatemala | Resolution JM-102-2011 of the Monetary Board | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Resolution JM-102-2011 of the Monetary Board includes some provisions regarding the obligations of financial institutions with respect to the administration of technological risk and confidentiality of information. Art. 24 requires that, when processing financial data outside the national territory, the institutions must previously have authorisation from the Superintendency of Banks and comply with the following requirements: allowing the Superintendency of Banks free access to its IT infrastructure, information systems, databases and facilities located outside the national territory, and providing it with the information it requires. |
| Guinea | Law No. L/2016/037/AN of 28 July 2016, on cybersecurity and personal data protection in the Republic of Guinea | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** According to Art. 28 of Part II of the Law L/2016/037/AN, the transfer of personal data is subject to prior authorization from the personal data protection authority. Any transfer of such data is subject to strict and regular control by the authorities with regard to their purposes. The authorization is always needeed, though, other conditions must also be fulfilled. A controller of personal data may only transfer such data to a third country if the state ensures a higher or equivalent level of protection of privacy, fundamental freedoms and rights of individuals with regard to the processing to which such data may be subject. |
| Guyana | Credit Reporting Act 2010 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 18 of the Credit Reporting Act 2010, credit reporting agencies may only store and retain in another country the data collected, provided they have the Bank of Guyana's approval. |
| Honduras | Tax Code - Decree No. 170-2016 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to Art. 63(3) of the Tax Code, taxpayers or the persons responsible for tax must conserve accounting books and special records, documents and other records of the taxable activity, electronic files, programmes, sub programmes and other records processed by electronic or computer systems, in an orderly manner and keep them in their fiscal domicile at the immediate disposal of the Finance Office's State Secretariat ('SEFIN'), the Customs Tax Superintendency, the Tax Administration or the Customs Administration, when requested or when duly accredited public servants show up at their fiscal domicile in order to request documentation or tax information. This information must be kept for a period of five years by taxpayers registered with the National Tax Registry and for a period of seven years in other cases. In addition, Art. 64(3) states that taxpayers must keep their accounting records at their fiscal domicile without prejudice to having contracted accounting services within the country. |
| Hong Kong | Circular to Licensed Corporations - Use of external electronic data storage | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Hong Kong's Securities and Futures Commission released a circular in October 2019 that requires banks and other regulated groups to store data locally or ensure their cloud provider guarantees it will hand over information on request. |
| Hong Kong | Personal Data (Privacy) Ordinance | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Section 33 of the Personal Data (Privacy) Ordinance, there are prohibitions against transfer of personal data to place outside Hong Kong except in specified circumstances. However, this Section has not yet come into operation. If the data is transferred by a data controller to its outsourcing agent situated outside Hong Kong for processing the data, the data user remains liable for all acts done by its agent in relation to the mishandling of the personal data. |

| | | |
|---|---|---|
| Hungary | Act L of 2013 on Electronic information security of state and local government organizations | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Under Section 3 of the Act L of 2013 on Electronic information security of state and local government organizations, data processing for certain institutions, including governmental bodies, National Bank, or local municipalities, must be provided from the territory of Hungary. |
| India | Request for Proposal (RFP) for Provisional Empanelment of Cloud Service Offerings of Cloud Service Providers (CSPs)<br><br>Guidelines for Government Departments on Contractual Terms Related to Cloud Services<br><br>Master Service Agreement: Procurement of Cloud Services | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** In 2015, India's Ministry of Electronics and Information Technology (MeitY) issued guidelines for a cloud computing empanelment process under which cloud computing service providers may be provisionally accredited as eligible for government procurement of cloud services. The guidelines require such providers to store all data in India to qualify for the accreditation.<br>In addition, Section 2.1.d of the Guidelines for Government Departments on Contractual Terms Related to Cloud Services requires that any government contracts contain a localization clause mandating that all government data residing in cloud storage networks is located on servers in India.<br>Furthermore, Section 1.17.4 of the Master Service Agreement: Procurement of Cloud Services outlines, among other things, that cloud service providers must offer cloud services to the purchaser from a MeitY-enrolled data centre which is located in India, the data must be stored within India, and must not be taken out of India without explicit approval by the purchaser. |
| India | Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015<br><br>Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017 | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** According to the Insurance Regulatory and Development Authority of India (IRDAI) Maintenance of Insurance Records Regulations, 2015 (Regulation 3(9)), "Insurers are required that [...] (ii) the records pertaining to policies issued and claims made in India (including the records held in electronic form) are held in data centres located and maintained in India." In addition, the 2017 Regulations on Outsourcing of Activities by Indian Insurers provide that Indian insurers, even in cases where they outsource their services outside India, must retain all original records in India. |
| India | Reserve Bank of India Directive | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** In April 2018, the Reserve Bank of India (RBI) issued a one-page directive stating that, within six months, all payment data held by payment companies should be held in local facilities. The Directive noted that this would help the RBI gain "unfettered supervisory access" to transaction data, which it needs to ensure proper monitoring.<br>Following a negative response from international payment companies such as MasterCard, Visa and American Express, the RBI has proposed (in "Frequently Asked Questions" of its website) to ease this restriction, so as to allow payment firms to store data offshore, as long as a copy was kept in India. The RBI has further clarified that for cross border transaction data consisting of a foreign component and domestic component, a copy of the domestic component may be stored abroad, if required.<br>With respect to processing of payment transactions outside India, the RBI requires that the data must be stored only in India after processing and should be deleted from systems abroad and brought back to India no later than 24 hours after processing. Any subsequent activity such as settlement processing after payment processing done outside India, this must be undertaken on a real time basis pursuant to which the data must be stored only in India.<br>The RBI has clarified that banks, especially foreign banks, can continue to store banking data abroad but in respect of domestic payment transactions, the data must be stored only in India. |

| | | |
|---|---|---|
| India | Companies (Accounts) Rules, 2014 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Rule 3(5) of the Companies (Accounts) Rules 2014 provides that if company books and papers (or back-ups of them) are kept electronically in any location, they must also be periodically stored on a server physically located in India. |
| India | Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Rule 7 of Information Technology Rules 2011 states that export of sensitive personal data or information within or outside India is permissible provided that the same standards of data protection required in India are adhered to, and that transfer is necessary for the performance of a lawful contract or has been consented to by the provider of the information. Sensitive personal information includes passwords, financial information such as bank account or credit/debit card details, sexual orientation, physical, mental health condition, biometric information, among others. |
| India | National Data Sharing and Accessibility Policy | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** India's National Data Sharing and Accessibility Policy requires that "non-sensitive data available either in digital or analog forms but generated using public funds" must be stored within the borders of India. The policy states that data belongs to the "agency/department/ministry/entity which collected them and reside in their IT enabled facility" (Section 10). |
| India | Public Records Act 1993 (No. 69 of 1993) | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Section 4 of the Public Records Act states that no person shall take or cause to be taken public records out of India without the prior approval of the Central Government, except if done for any offical purpose. |
| India | Licence Agreement for Unified Licence | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Under Condition 39.23(viii) of the Unified Licence Agreement granted by the Department of Telecommunications, licensees are not permitted to transfer "subscriber accounting information" (except for roaming and related billing purposes) or "user information" (except if pertaining to foreign subscribers using an Indian Operator's network while roaming, and International Private Leased Circuit subscribers) to any person or place outside of India. "User information" is not defined by Indian telecommunications law and the requirements do not restrict financial disclosures imposed by statute. Condition 39.23(iii) prohibits the transfer of domestic technical network details to any place outside of India. |

| | | |
|---|---|---|
| Indonesia | OJK Regulation (POJK) No. 11/ POJK.03/2022 regarding the Implementation of Information Technology by Commercial Banks<br><br>POJK No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** In accordance with Art. 35 of OJK Regulation (POJK) No. 11/ POJK.03/2022, banks are required to place their electronic systems in data centers and disaster recovery centers in Indonesia. Yet, banks may place them outside Indonesia upon obtaining authorization from the Financial Services Authority (OJK). According to Art. 36, banks may apply for an authorization provided that they:<br>- meet the regulatory provisions on the use of IT service providers in IT implementation;<br>- submit the results of the country risk analysis;<br>- ensure that the placement of the electronic systems in data centers and/or disaster recovery centers outside Indonesia does not diminish the effectiveness of OJK's supervision as demonstrated by a statement letter;<br>- ensure that information regarding the bank's confidentiality is only disclosed on the condition that such disclosure complies with the provisions of the statutory regulations in Indonesia, as evidenced by the cooperation agreement between the bank and the IT service provider;<br>- ensure that the written agreement with the IT service provider contains a choice of law clause;<br>- submit a no-objection letter from the supervisory authority of the IT service provider outside Indonesia that OJK can conduct inspections on the IT service provider;<br>- submit a statement letter that the bank shall periodically submit the results of assessments conducted by the bank office(s) outside Indonesia on the application of risk management on the IT service provider;<br>- ensure that the placement plan of the electronic systems in data centers and/or disaster recovery centers outside Indonesia delivers more benefits than the costs for the bank; and<br>- submit the bank's plan to improve the bank's human resources capacity, both in IT implementation and in business transactions or products offered.<br>In addition, according to Art. 39, banks are required to process IT-based transactions within the Indonesian territory. However, the processing of IT-based transactions by the IT service providers outside Indonesia can be carried out provided that the bank has obtained authorization from OJK. Banks may apply for an authorization on the condition that:<br>- IT service providers comply with the prudential principle, with the regulatory provisions on the IT service providers in IT implementation, and take heed of consumer protection.<br>- the supporting documents for financial administration for transactions conducted at the bank offices in Indonesia are administered at the bank offices in Indonesia; and<br>- the bank's business plan demonstrates efforts to increase the bank's role in developing Indonesia's economy.<br>OJK Regulation (POJK) No. 11/POJK.03/2022 revoked and declared null and void OJK Regulation (POJK) No. 38/POJK.03/2016, which already required foreign banks and payments networks to locate data centers and process electronic transactions in Indonesia. |
| Indonesia | Regulation No. 4/POJK.05/2021 - Implementation of Risk Management in the Use of Information Technology by Nonbank Financial Services Institutions | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Under Art. 23 Reg No. 4/05/2021, non-bank financial institutions are obligated to place their data centre and/or disaster recovery centre within the territory of Indonesia. An exemption of this obligation may only be applicable after obtaining a prior approval from the Financial Services Authority (Otoritas Jasa Keuangan, OJK) and only for certain purposes of electronic system. |

| | | |
|---|---|---|
| Indonesia | Bank Indonesia Regulation No. 22/23/PBI/2020 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 35 of Bank Indonesia Regulation No. 22/23/PBI/2020 requires domestic processing of initiation-authorization-clearing-settlements phases of payment transactions for instruments issued by Indonesia's payment service provider and conducted within the territory of the Republic of Indonesia. Indonesia opens the possibility of such payment transactions to be processed outside of Indonesian territory for the purpose of global reconciliation, integrated risk management system/anti-money laundering. However, this is subject to Bank Indonesia's approval. |
| Indonesia | OJK Circular Letter No. 14/SEOJK.07/2014 | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Art. 2 of the Financial Service Authority (OJK) Circular Letter No. 14/SEOJK.07/2014 stipulates that financial service institutions should not disclose the data of its customer to a third party unless they get consent from the data owner. The consent should be expressed in writing. |
| Indonesia | Government Regulation No. 46/2014 | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** Art. 21 of Government Regulation No. 46/2020 mandates that the health data should be stored in Indonesia. |
| Indonesia | Minister of Communication and Informatics Regulation No. 20 of 2016 regarding Protection of Personal Data in Electronic Systems<br><br>Government Regulation No. 71/2019 regarding the Provision of Electronic System and Transaction | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The Ministry of Communication and Informatics (MOCI) Regulation No. 20 of 2016 stipulates that consent from the data subject is necessary for the transfer of data, such consent must also be in Bahasa Indonesia (or in bilingual format) and collected online or by paper hard copies. The Regulation also mandates that personal data that is electronically stored should be encrypted.<br>Under Government Regulation No. 71/2019, consent must be obtained from data subjects for cross-border transfers of personal data. Such consent must be “lawful consent”, i.e. consent that is delivered explicitly, cannot be concealed, and is not based on error, negligence or coercion. |
| Indonesia | Law No. 27 of 2022 regarding Personal Data Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 56 of Law No. 27 regarding Personal Data Protection allows the cross-border transfer of personal data from a controller to a controller and/or processor outside the jurisdiction of Indonesia if recipient country has an adequate level of protection. If the country is not adequate, the controller must ensure an adequate and binding personal data protection. Alternatively, the controller must obtain the consent of the data subject. |
| Indonesia | Regulation No. 8 of 2021 on Implementing Guideline of Physical Market Trading of Crypto Assets in the Futures Exchange | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** Under Arts. 7, 11, 14 and 18 of Bappebti Reg No. 8/2021, the stakeholders of crypto asset trade (i.e., futures market, futures clearing institution, crypto asset physical trader, and crypto asset depository manager) are obligated to place their disaster recovery center as well as a server or cloud server within Indonesia. The disaster recovery center must be located within a maximum distance of 20 km from the main server. A crypto asset is defined as a digitally intangible commodity, using cryptography, information-technology network, and a distributed ledger to implement the creation of new units, verify transactions, and secure transactions without any intervention from any third party. |
| Indonesia | Government Regulation No. 80/2019 | **Category:** Conditional flow regime<br>**Sector:** Other<br>**Description:** Art. 59 of the Government Regulation No. 80/2019 states that personal data collected in e-commerce activities cannot be sent overseas unless the relevant Ministries confirm that the foreign country has the same level of personal data protection standard as Indonesia. |

| | | |
|---|---|---|
| Indonesia | Regulation of the Government of the Republic of Indonesia No. 71 of 2019 on Electronic System and Transaction Operations<br><br>Government Regulation No. 82 of 2012 on Electronic System and Transaction Operations | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 20 of Regulation No. 71 provides that the public electronic system operators (ESOs) are required to manage, process, and/or store electronic systems and electronic data in the territory of Indonesia, except if the technology is not yet available. Private ESOs can manage, process, and/or store electronic systems and electronic data in Indonesia and/or outside the country (Art. 21). However, if management is carried out outside, it must ensure the effectiveness of supervision by the ministry, etc.<br>Art. 1 contains several key definitions:<br>- Electronic system: a set of electronic equipment and procedures which have the function to prepare, collect, process, analyze, store, display, announce, deliver and/or disseminate electronic information.<br>- ESO: any persons, state administrators, business entities and the public that provide, manage and/or operate an electronic system individually or jointly to electronic system users for its own interests and/or the interests of another party.<br>- Public ESO: an electronic system operation by a state administrator agency or institutions appointed by a state administrator agency.<br>- Private ESO: an electronic system operation by a person, business entity and the public.<br>With the entry into force of Regulation No. 71, Regulation No. 82 was repealed and declared null and void. Under Art. 17 of Regulation No. 82, ESOs for public services had to establish data centres and a disaster recovery centre in Indonesia impacting many private sector companies. |
| Indonesia | Regulation of the Government of the Republic of Indonesia No. 71 of 2019 on Electronic System and Transaction Operations<br><br>Regulation of the Minister of Communications and Informatics of the Republic of Indonesia No. 5 of 2020 on Private Electronic System Operators (“Regulation 5”) | **Category:** Conditional flow regime<br>**Sector:** Telecom sector<br>**Description:** Art. 21 of Government Regulation No. 71/2019 states that the electronic systems operators for private scope can store and process the electronic transaction data outside Indonesia under certain conditions. The companies must ensure that their electronic systems and data are accessible to the Indonesian authority for supervision and law enforcement. ESOs for private scope are defined as the intended subject being a Person, Business Entity, or community consisting of (i) ESO that are regulated and supervised by the relevant Ministry or Institution based on laws and regulations, and (ii) ESO which own portals, websites, or applications within the internet network, whose electronic system is used in and/or offered in Indonesian territory, and is used, among others, to sell, manage and/or operate offers and/or trade goods and/or services and search engine. Regulation of Minister of Communication and Informatics No. 5 of 2020 on Private Electronic System Operators (“Regulation 5”) implements Government Regulation No. 71/2019. |
| Italy | Presidential Decree No. 633 of 1972 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Art. 39 of the Presidential Decree No. 633 of 1972 states that electric archives related to accounting data for VAT declarations may be kept in a foreign country only if some kind of convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation. Therefore, such limitation does not apply intra-EU. |

| | | |
|---|---|---|
| Jamaica | The Data Protection Act, 2020 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Section 1 of Art. 31 of The Data Protection Act, personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. However, according to Section 3 of Art. 31, the aforementioned condition is not necessary for a transfer that falls within any of the cases specified in subsection 4, including:<br>- The interested individual consents to the transfer;<br>- The transfer is necessary for the performance of a contract between the data subject and the data processor;<br>- The transfer is necessary for reasons of substantial public interest;<br>- The transfer is necessary for the purpose of, or in connection with, any legal proceedings (including possible legal proceedings);<br>- The transfer is necessary to protect the vital interests of the data subject;<br>- The transfer is made on terms that are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects;<br>- The Commissioner has authorized the transfer to be made in a manner that ensures adequate safeguards for the rights and freedoms of data subjects;<br>- The transfer is necessary for the purposes of national security or the prevention, detection, or investigation of criminal offenses. |
| Japan | Common Standards for Information Security Measures for Government Agencies | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) “Common Standards for Information Security Measures for Government Agencies” allows for government agencies to make use of systems that are "isolated" from the internet if necessary. Information on the agencies affected is not readily available. This policy effectively involves the localisation of data used by the public services concerned. |
| Japan | Guidelines on Security Management of Information System and Services Handling Medical Information | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** The Guidelines on Security Management of Information System and Services Handling Medical Information provide that information systems for the handling of medical data must be located in the territory of Japan so that in the event of an emergency, Japanese governmental authorities can enforce their power to collect information or issue administrative orders. Although this is not a mandatory requirement based on a specific law, it is reported that some medical institutions have requested that service providers maintain servers inside Japan to comply with these Guidelines. |

| | | |
|---|---|---|
| Japan | Act on the Protection of Personal Information (Act No. 57 of 2003)<br><br>Enforcement Rules for the Act on the Protection of Personal Information | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI) did not originally restrict the transfer of personal information to foreign countries, but amendments enacted in 2015 and which took effect in May 2017 added restrictions on cross-border data flows. The amended APPI prescribes three types of legitimate transfers of personal information to a third party in a foreign country under Art. 24: (1) transfers to a country that the Personal Information Protection Commission (PPC) has designated as having an acceptable level of data protection; (2) transfers to a third party in a foreign country in circumstances in which actions have been taken to ensure the same level of data protection as in Japan (such as entering into a data transfer agreement imposing obligations on the transferee meeting the requirements of the APPI); or (3) transfers with the data subject's consent.<br>Under the Enforcement Rules for the APPI (promulgated in 2016), as for (2), Art. 11 specifies that it means: "(i) a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method or (ii) a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information." To date, the only PPC-recognized international framework is the APEC Cross-Border Privacy Rules System. |
| Jordan | Law No. 24 of 2023 - Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 15 of the Personal Data Protection Law provides that any cross-border transaction of personal information must be transferred to a party that has a sufficient level of data protection. The level of protection afforded to a data recipient is equivalent to that imposed by Jordanian laws and regulations, except in the following cases: judicial cooperation is established under international conventions and treaties; international cooperation in the field of combating crimes; data exchange is essential for patient treatment; data exchange is related to epidemiological and health disasters or public health related to Jordan; the data subject has approved the transfer of data after being made aware that the level of protection outside the jurisdiction is not equivalent to the level imposed by Jordanian laws and regulations; and transfer of funds abroad. |
| Kazakhstan | Law of the Republic of Kazakhstan of 21 May 2013 No. 94-V on Personal Data and Its Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** In addition to the legal requirement of local processing of personal data in Kazakhstan introduced in 2015 in the Personal Data Law (Art. 12.2), pursuant to Art. 16.2 of the Law, a copy of personal data may only be transferred from Kazakhstan to a foreign country (including for purposes of processing) without prior permission from the personal data subject only if the recipient of the personal data is located in a country that protects personal data (at either the national level (by adopting national laws and regulations) or the international level (through international treaties). Pursuant to Art. 16.3 of the Personal Data Law, if no such protection is available, cross-border transfers of personal data are only possible if:<br>- The subject gives specific consent;<br>- In cases specified by international treaties ratified by Kazakhstan;<br>- In cases stipulated in the laws of Kazakhstan in order to protect the constitutional order, public order, rights and freedoms of an individual and a citizen, and public health and morality; and<br>- In the case of the protection of the constitutional rights of an individual and citizen, where getting the consent of the subject or their legal representative is impossible.<br>It is reported that national legislation does not specify a list of countries to which transfer of data is prohibited, nor are there any criteria listed for determining the countries that provide a proper level of protection of personal data. |

| | | |
|---|---|---|
| Kazakhstan | Law of the Republic of Kazakhstan of 21 May 2013 No. 94-V on Personal Data and Its Protection<br><br>Decree of the Government of the Republic of Kazakhstan of 3 September 2013 No. 909 on Approval of the Rules for the Implementation by the Owner and/or Operator, and a Third Party of Measures on Protection of Personal Data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Pursuant to Art. 12.2 of the Personal Data Law, personal data should be stored in a database located on the territory of Kazakhstan by the owner and/or operator, as well as third parties. In addition, in accordance with Subparagraph 4) of Art. 26 of the Personal Data Law, the Government of Kazakhstan decreed the approval of the Rules for the Implementation by the Owner and/or Operator, and a Third Party of Measures on Protection of Personal Data (Decree No. 909). In 2021, the Rules were supplemented with the provision that the collection and processing of personal data "of limited access" is carried out through informatization objects located on the territory of Kazakhstan. In accordance with paragraph 10 of these Rules, it is necessary not only to store personal data in Kazakhstan, but to collect and process personal data in Kazakhstan. It is reported that there is no clear distinction between publicly accessible data and data "of limited access". It is presumed that all personal data is of restricted access (including last name, first name, patronymic name, year, date of birth, nationality, information about the place of residence, individual identification number ('IIN'), details of identity documents), until the data subject makes them publicly accessible. |
| Kazakhstan | Law of the Republic of Kazakhstan No. 418-V ZRK about informatization<br><br>Acting Chairman of the Republic of Kazakhstan Agency for Informatization and Communication Order No. 88-b of 5 April 2005 on the Approval of Regulations for the Allocation of Domain Space in the Kazakhstan Segment of the Internet | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** Art. 56-1 of the Law on Informatization requires that internet resources with ".kz" and ".қaz" domains must be hosted on hardware and software complexes located in Kazakhstan. In other words, an internet resource (website, web application, web service) using a ".kz" or ".қaz" domain must be hosted on a server (owned / rented / cloud hosted / VDS hosted / virtually hosted) in a data center (server / office) located in Kazakhstan. The server must also be connected to a Kazakh internet provider and use a (dedicated or shared) Kazakhstan IP address.<br>A similar requirement was in place since 2005, as established in Clauses 7 and 8 of the Regulations for the Allocation of Domain Space in the Kazakhstan Segment of the Internet. These clauses provided that an application for domain name registration may be refused, or registration may be cancelled, if the domain servers were not located inside Kazakhstan. |
| Kazakhstan | Law of the Republic of Kazakhstan on Communication | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 21 of the Law of the Republic of Kazakhstan on Communications stipulates that operators of communication networks of all categories included in the unified telecommunications network of the Republic of Kazakhstan shall be obliged to create at their own expense a system of centralized management of their networks, which must be located on the territory of the Republic of Kazakhstan. |
| Kazakhstan | Resolution of the Government of the Republic of Kazakhstan No. 246 | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Paragraph 6-1 of Resolution No. 246 prohibits the storage of telecommunication subscriber information outside the country. |

| | | |
|---|---|---|
| Kenya | Data Protection Act (No. 24 of 2019)<br><br>Data Protection (General) Regulations, 2021<br><br>Computer Misuse and Cybercrimes Act No. 5 of 2018 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Section 50 of the Data Protection Act provides that the Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, processing of a certain nature that should only be affected through a server or data center located in Kenya. Regulation 26(1) of the Data Protection (General) Regulations states that pursuant to Section 50 of the Act, a data controller or data processor who processes personal data for the purposes of strategic interests of the state outlined in Regulation 26(2) should: process such personal data through a server and data center located in Kenya; or store at least one serving copy of the concerned personal data in a data center located in Kenya (whereby no definitions have been provided for the term 'serving copy'). In accordance with Regulation 26(2) of the General Regulations, the strategic purposes contemplated in Regulation 26(1) include the processing of personal data for:<br>- administering the civil registration and legal identity management systems;<br>- facilitating the conduct of elections for the representation of the people under the constitution;<br>- overseeing any system for administering public finances by any state organ;<br>- running any system designated as a protected computer system in terms of Section 20 of the Computer Misuse and Cybercrimes Act;<br>- offering any form of early childhood education and basic education under the Basic Education Act No. 14 of 2013; and<br>- providing primary or secondary healthcare for a data subject in the country.<br>Under the Computer Misuse and Cybercrimes Act, a protected system is defined as a computer system used directly in connection with, or necessary for:<br>- the security, defense, or international relations of Kenya;<br>- the existence or identification of a confidential source of information relating to the enforcement of a criminal law;<br>- the provision of services directly related to communications infrastructure, banking, and financial services, payment and settlement systems, and instruments, public utilities, or public transportation, including government services delivered electronically;<br>- the protection of public safety, including systems related to essential emergency services, such as police, civil defense, and medical services;<br>- the provision of national registration systems; or<br>- such other systems as may be designated relating to the security, defense, or international relations of Kenya, critical information, communications, business, or transport infrastructure, and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication, and technology. |
| Kenya | Data Protection Act No. 24 of 2019 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 48 of the Data Protection Act No. 24 of 2019 states that a data controller or data processor may transfer personal data to another country only where the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data. Alternatively, data can be transferred if the transfer is necessary for: the performance of a contract; for any matter of public interest; for the establishment, exercise or defence of a legal claim; in order to protect the vital interests of the data subject or of other persons; or for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.<br>Art. 49 highlights safeguards prior to transfer of personal data out of Kenya, which include: (1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards; (2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests; (3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined. |

| | | |
|---|---|---|
| Kenya | National Information, Communications and Technology (ICT) Policy Guidelines of 2020 | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** The National ICT Policy Guidelines (paragraph 4.4) provide that all arms of government build, deploy, operate and manage locally built back-end and front-end systems. The Guidelines also require that all Kenyan data remains in Kenya and is stored safely and in a manner that protects the privacy of citizens to the utmost. |
| Korea | Act on the Development of Cloud Computing and Protection of Its Users | **Category:** Conditional flow regime<br>**Sector:** Cloud-computing sector<br>**Description:** Per Art. 27 of Act on the Development of Cloud Computing and Protection of Its Users, generally, "no cloud computing service provider shall provide any user information to a third party or use user information for any purpose other than for the purpose of providing services, without the relevant user's consent." This conditional flow regime has been in place since 2015. |
| Korea | Infrastructure requirement | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** It is reported that a cloud server that stores patient electronic medical records created by a hospital must be located in South Korea. Specifically, the Standard on Facilities and Equipment for Managing and Storing Hospital-Generated Electronic Medical Records, establishes that official notification will be issued by the Ministry of Health and Welfare every three years stating the requirements for servers (including back-up servers) on which hospital-generated electronic medical records must be stored. Currently, these servers must be physically located in South Korea and it is not permissible to access medical records from an overseas location. |
| Korea | Regulations on Electronic Financial Supervisory Regulations | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** The Electronic Financial Supervisory Regulations imposes a local processing requirement for financial services who intend to utilize cloud services for credit information and unique identification information (e.g. resident registration number, driver's licence number, passport number and alien registration number) (Art. 14-2). Financial companies and electronic financial business operators are required to use cloud systems located in Korea for processing of personal credit information and unique identification information. This provision was inserted as part of an amendment in December of 2018. |
| Korea | Credit Information Use and Protection Act | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** According to Art. 32 of the Credit Information Act, the credit information provider/user should obtain prior consent of the customer in writing or by other reliable means each time it provides to a third party or uses personal credit information (including any personal identifiable information) of a customer. When the credit information provider/user obtains consent to the provision (i.e. sharing) and utilisation of personal credit information, it should notify the customer of: the recipient of the information; the purpose of provision; the content of information; the duration of maintenance; and use by the recipient. Furthermore, a separate explanation to the customer is required with respect to the mandatory items of personal data that must be provided for the provision of the services and other optional items of personal data, and consent obtained. In such cases, as to the mandatory items, the credit information provider/user must explain their relevance to the service provision. Art. 32 requires the credit information provider/user to notify the customer that they may opt not to consent to the provision of any optional data that may be collected.<br>The Act established that financial institutions are required to obtain consent of individuals only if the use of personal information "conflict[s] with the original purpose of the collection." Thus, under this regime, a financial institution may "entrust" personal information to a third party but may not "supply" it. Supplying and entrusting are terms of art under the Act. "Supplying" means transferring personal information for the transferee's own purpose whereas "entrusting" means transferring personal information to a third party to help carry out the purpose of the original data collection. |

| | | |
|---|---|---|
| Korea | Personal Information Protection Act No. 10465 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 28-8 of the Personal Information Protection Act prohibits any transfer of personal information overseas by a personal information manager unless it is in any of the following cases: (i) where a separate consent for overseas transfer has been obtained from the data subject; (ii) where there exist special provisions in a statute, a treaty or other international conventions to which the Republic of Korea is a party; or (iii) where it is necessary to delegate the processing of, or retain, personal information in order to execute and perform a contract with a data subject, and the matters to be informed to the data subject when obtaining his/her consent to overseas transfer have been informed to the data subject or have been disclosed in the personal information manager's privacy policy; (iv) where the recipient of personal information has obtained certification determined and publicly notified by the Personal Information Protection Commission (PIPC) and has implemented certain measures to protect personal information; or (v) where the PIPC has recognized that the country or the international organization to where the personal information is transferred has the personal information protection system, etc. that are substantially equal to the level of those under the Personal Information Protection Act. The personal information manager shall also take certain technical, managerial and physical protection measures. |
| Korea | Act on the Protection, Use, Etc. of Location Information | **Category:** Local processing requirement<br>**Sector:** Maps sector<br>**Description:** Per Art. 5 of the Act on the Protection, Use, Etc. of Location Information, any person who intends to engage in location information business shall obtain permission from the Korea Communications Commission. Even if permitted to do such business, location information providers or location-based service providers cannot collect location information of individuals without individual's' consent under Art. 18. These restrictions have been in place since 2005.<br>It is reported that, although a supplier may export location information once acquiring a permit, Korea has never approved such a permit despite numerous applications by foreign suppliers over the past decade. |
| Korea | Act on the Establishment, Management of Spatial Data | **Category:** Conditional flow regime<br>**Sector:** Maps sector<br>**Description:** Art. 16 of Act on the Establishment, Management of Spatial Data provides that geographical data related to maps or photos produced for the purpose of a survey cannot be transferred abroad except with the permission of the Minister of Land, Infrastructure and Transport. This provision has been in place since 2014. |
| Kuwait | Data Privacy Protection Regulation, No. 42 of 2021 | **Category:** Conditional flow regime<br>**Sector:** Telecom sector<br>**Description:** The Data Privacy Protection Regulation of 2021 defines "data collection and processing" broadly, including also transmission of data. Data processing, and therefore also data transfer across borders, is lawful under limited circumstances, including with the consent of the data subject or in case of necessity to comply with a legal obligation (Art. 5). Firms shall notify data subjects if their data is transferred abroad (Art. 6.10), providing also information about how long and where data will be stored overseas (Art. 6.8). The Regulation is not applicable to security agencies. |

| | | |
|---|---|---|
| Kyrgyz Republic | Law of the Kyrgyz Republic of 14 April 2008 No. 58 on Personal Information | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Pursuant to Art. 25 of the Law No. 58 on Personal Information, the cross-border transfer of personal data is permitted in the case where a personal data holder located within the Kyrgyz jurisdiction transfers such databases on the basis of an international agreement between the parties, according to which the receiving party provides an adequate level of protection of the rights and freedoms of personal data subjects. If a certain country does not provide an adequate level of protection of personal data, personal data may be transferred in the following cases:<br>- with the consent of a data subject for such transfer;<br>- where such a transfer is necessary for the protection of a data subject's interest; or<br>- where personal data is contained in a publicly available array of personal data.<br>It should be emphasized that in the case of transferring personal data via the internet, the personal data holder transferring such data shall ensure that data is transferred with the necessary means of protection. |
| Lao | Law on Electronic Data Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The Law on Electronic Data Protection specifies that the delivery or transfer of data must be performed as follows:<br>- with the consent of the data subject and guarantee that the transferee can protect such data;<br>- with the encryption of important information, such as financial, accounting, and investment data and with the electronic certificate issued by the Ministry of Posts and Telecommunication (Art. 25);<br>- without forging the source of data sent or transferred;<br>- that the transfer must be in accordance with the agreement of the transferee and transferor; and<br>- that the transfer must be stopped upon refusal by transferee.<br>The transfer of private data outside of Lao PDR is subject to the express consent of data subject and compliance with law (Art. 17). |
| Lao | Decree on the Management and Use of Internet and Domain Name of the Lao PDR | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** The political parties and government organizations having their own website must use the Domain Name ".la" and must store the information in the land system computer which uses the Internet Protocol of the National Internet Center located in Lao PDR according to Art. 10 of the Decree on the Management and Use of Internet and Domain Name of the Lao PDR. |
| Lesotho | Data Protection Act, 2011 - Act No. 5 of 2012 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Lesotho's data protection law allows cross-border data transfers, which are regulated as transfer of personal information outside Lesotho under Section 52 of the Data Protection Act of 2012.<br>The transfer of personal information abroad is permitted when the laws of the destination country are substantially similar to the information protection principles under Data Protection Act of Lesotho, or one of the other conditions are met (e.g., the data subject consents to the transfer or the transfer is necessary for the performance of contract between the data subject and data controller). Private sector safeguards, such as binding corporate rules, may also be put in place. |
| Liberia | Regulations Concerning the Licensing & Operations of Electronic Payment (E-Payment) Services (No. CBL/RSD/003/2020) | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Regulation 9.0 of Regulations No. CBL/RSD/003/2020 provides that IT and security systems of e-payment service providers should be hosted locally to provide ease of support and guarantee data ownership; however, if the system is hosted in another jurisdiction, licensed institutions shall ensure that the information requested is provided promptly and that the Central Bank of Liberia has unfettered access to reports generated by the system. |

| | | |
|---|---|---|
| Libya | Law No. 6-2022 on Electronic Transactions | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 78 of Law No. 6/2022 on Electronic Transactions, the transfer of personal data to a foreign country is only allowed if the appropriate level of data protection is considered, particularly the nature and source of the personal data and the purpose and duration of the transfer. Also, the applicable international obligations and laws and national data protection procedures of the country to which the data is transferred must be considered. |
| Luxembourg | Law of 19 December 2002 on the register of commerce and companies and the annual accounts of companies, amending the Commercial Code | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to the Commercial Code, Book I, Art. 8, the books, accounts and supporting documents relating to offices and branches of foreign firms based in Luxembourg must be kept in Luxembourg. Accounting documents may be kept either in electronic format or in paper format. |
| Madagascar | Law No. 2014 - 038 of 9 January 2015 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 20, any personal data may be transferred only to countries that have legislation ensuring a level of protection for individuals similar to that provided by Malagasy law. Exceptionally, and with the agreement of the Malagasy Commission on Information Technology and Liberties (CMIL), the transfer of personal data is possible when the data controller presents sufficient guarantees for the protection of privacy and the fundamental rights and freedoms of individuals. In addition, it is also permitted when the individual concerned gives his/her full consent, when it is in his/her interest or for the performance of a contract concerning that individual.<br>The processing of sensitive data (racial origin, biometric data, genetic data, political opinions, religious or other beliefs, trade union membership and data relating to health or sex life) is prohibited. Derogations exist when guarantees of appropriate processing are provided to the Malagasy Commission for Computer Liberties (Art. 18). |
| Malawi | Malawi National Health Information System Policy of September 2015 | **Category:** Local processing requirement<br>**Sector:** Health sector<br>**Description:** Section 12.4 of the Malawi National Health Information System Policy provides a requirement for any health related data whether physical or electronic to be stored only within the borders of Malawi except for the purpose of continuation of care. Section 14.1 ascribes ownership of any health related data to the Ministry of Health. This policy was elaborated for the health sector of Malawi, i.e. public and private. The stipulations therein therefore apply to all public and private health facilities alike (Section 2). |
| Malaysia | Companies Act 1965 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Under Section 167(3) of the Companies Act 1965, accounting and other such financial records pertaining to operations in Malaysia must be stored at the company's registered address or at any other such place in Malaysia. Section 167(5) of the Companies Act states that if records are kept at a place outside of Malaysia, pursuant to Section 167(4) regarding operations outside of Malaysia, these records must be made available in Malaysia if required by the Registrar. |
| Malaysia | Income Tax Act 1967 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Section 82(8) of the Income Tax Act 1967 states that all records that relate to any business in Malaysia shall be kept and retained in Malaysia. |

| | | |
|---|---|---|
| Malaysia | Goods and Services Tax Act 2014<br><br>Guide to Goods and Services Tax | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Section 36(2)(c) of the Goods and Services Tax Act creates a duty to keep records described in Section 36(1) in Malaysia, except as otherwise approved by the Director-General of the Royal Malaysian Customs Department. These include all records of goods and services provided by a taxable person, all imports records by the same, and, as per paragraph 133(c) of the Guide to Goods and Services Tax, any other supporting documents such as contracts or price quotations that affect or may affect said person's liability under the Act. Paragraph 134(b) of the Guide states that the requirements cover documents in electronic form.<br>Section 36(6) of the Act extends the requirements to certain non-taxable persons. Paragraph 135 of the Guide specifies that these include:<br>- any person who has ceased to be a taxable person and has made or may make a bad debt relief claim;<br>- imported services supplied to a recipient who is a non-taxable person for the purposes of business;<br>- goods of a taxable person sold by a non-taxable person to recover any debt owed by the taxable person;<br>- supply by auctioneer, who is a non-taxable person, in his own name on behalf of the principal/owner of the goods who is a taxable person; and<br>- a non-taxable person in Malaysia who receives goods in the course or furtherance of business, from an approved toll manufacturer. |
| Malaysia | Personal Data Protection Act 2010 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 129(1) of the Personal Data Protection Act (PDPA) prohibits a data user from transferring the personal data of a data subject to a place outside of Malaysia unless to places specified by the Minister, upon the recommendation of the Personal Data Protection Commissioner, by notification published in the Gazette. The Minister may specify such places that have any law in force which is substantially similar to the PDPA, serves the same purpose as the PDPA, or ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA. Section 129(3) of the PDPA provides exceptions whereby a data user may transfer any personal data to a place outside Malaysia if:<br>- the data subject has given their consent to the transfer;<br>- the transfer is necessary for the performance of a contract between the data subject and the data user;<br>- the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which: is entered into at the request of the data subject; or is in the interests of the data subject;<br>- the transfer is for the purpose of any legal proceedings, obtaining legal advice or for establishing, exercising, or defending legal rights;<br>- the data user has reasonable grounds for believing that in all circumstances of the case: the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; and where it is practicable to obtain consent, the data subject would have given their consent;<br>- the data user has taken all reasonable precautions and exercised all due diligence to ensure that personal data will not be processed in any manner which if that place were Malaysia, would be a contravention of the PDPA;<br>- the transfer is necessary in order to protect the vital interests of the data subject; or<br>- the transfer is necessary as being in the public interest in circumstances as determined by the Minister. |

| | | |
|---|---|---|
| Mali | Law No. 2013-015 on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 11 of Law No. 2013-015, Mali authorizes the transfer of personal data to a foreign State when:<br>- The receiving State ensures a sufficient level of protection of individuals, indicated by the Authority in charge of the protection of personal data, due to its domestic legislation or commitments made at the international level and that these measures are effectively implemented.<br>- By decision of the Authority in charge of the protection of personal data, when the transfer and processing by the recipient of the personal data ensures a sufficient level of protection of privacy, as well as of the fundamental rights and freedoms of individuals, in particular, due to the contractual clauses or internal rules to which it is subject. |
| Mali | Law No. 2013-015 on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Pursuant to Art. 9 of Law No. 2013-015, the processing of sensitive data, understood as any data of a personal nature relating to religious, philosophical, political, or trade union opinions or activities, sex, race, health, social measures, prosecutions, and criminal or administrative charges, is prohibited. However, sensitive data may be processed with appropriate safeguards defined by the Authority in charge of personal data protection if the data is necessary or used to safeguard the person's life, used by a non-profit organisation, or in the context of a judicial action.<br>Processing of personal data is defined as any operation or set of operations carried out by means of automated or non-automated processes and applied to data, such as collecting, exploiting, recording, organizing, storing, adapting, modifying, retrieving, saving, copying, consulting, using, communicating by transmission, disseminating or otherwise making available, bringing together or interconnecting, as well as blocking, encrypting, deleting or destroying personal data. |
| Malta | Virtual Financial Assets Act<br><br>Virtual Financial Assets Rulebook (Chapter 3 of the Virtual Financial Assets Rules for VFA Services Providers) | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** The Malta Financial Services Authority has imposed in R3-3.5.2.1.6 of its Virtual Financial Assets Rulebook (Chapter 3 of the Virtual Financial Assets Rules for VFA Services Providers) a requirement for licence holders to ensure that its IT infrastructure is located in Malta, and/or any other European Economic Area member state, and/or any other third country jurisdiction wherein the Authority is satisfied that the IT infrastructure ensures the integrity and security of any data stored therein; availability, traceability and accessibility of data; and privacy and confidentiality. This shall apply to virtual financial asset (VFA) service providers licensed in terms of the Virtual Financial Assets Act and applicants seeking licensing as VFA service providers under the Act, as applicable. |
| Malta | Technical Infrastructure hosting Gaming and Control Systems Guidelines | **Category:** Local storage requirement<br>**Sector:** Gambling sector<br>**Description:** The Malta Gaming Authority imposes real-time replication in a local server of "regulatory data" in the gaming sector in their Technical Infrastructure Guidelines (Guideline 3.2). Regulatory data is composed of player details, financial transactions, and game-play transactions. |

| | | |
|---|---|---|
| Mauritania | Law No. 2017-020 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Law No. 2017-020 provides that the controller may transfer personal data to a third country only if that country ensures an adequate level of protection (Art. 20). The Personal Data Protection Authority shall publish and maintain a list of states that it considers to provide an adequate level of protection (Art. 21). If the country is not included in the list of adequate countries, the controller must first inform the Authority. Moreover, Art. 24 specifies that the data controller may transfer personal data to a third country that does not meet the requirements of Art. 21, if the transfer is one-off, not massive and the person to whom the data relates has expressly consented to its transfer, or if the transfer is necessary for any of the following purposes:<br>- to safeguard the life of that person.<br>- to protect the public interest.<br>- to comply with obligations to establish, exercise or defend a legal claim.<br>- the performance of a contract between the controller and the data subject.<br>Lastly, the Authority may authorize, on the basis of a duly motivated request, a transfer or a set of transfers of data to a third country that does not ensure an adequate level of protection, when the data controller offers sufficient guarantees with regard to the provisions of this law, including through contractual clauses (Art. 25). |
| Mauritius | Act 20/2017, Data protection Act | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Section 36(1) of the Data Protection Act, a data controller may transfer data abroad only under certain conditions. These include the compliance with appropriate safeguards, the explicit consent of the data subject and other cases of necessity of the transfer.<br>Under Section 36(4) of the Data Protection Act, the Data Protection Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as the Data Commissioner may determine. It is reported that the authorities are yet to enforce these principles. |
| Mexico | Provisions on Electronic Payment Fund Institutions | **Category:** Conditional flow regime<br>**Sector:** Cloud-computing sector<br>**Description:** There are concerns that Art. 50 of the Provisions on Electronic Payment Fund Institutions might force firms to choose only cloud providers based in Mexico, thus indirectly imposing a local data processing requirement. The law requires electronic payment fund institutions to use secondary cloud service provided by a company that is not subject to a different jurisdiction. That would mean that the secondary cloud provider would need to be subject to the Mexican jurisdiction. |
| Mexico | Federal Law on the Protection of Personal Data in Possession of Individuals | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Consent is necessary for data transfer of personal data across borders on the basis of Arts. 6, 8, and 9 of the Federal Law on the Protection of Personal Data in Possession of Individuals. Moreover, pursuant to Art. 37 of the law, domestic and international transfers of personal data may be carried out without the consent of the data subject under certain exceptions including, among others: the necessity of the transfer for medical diagnosis or prevention, health care delivery, medical treatment or health services management; the transfer to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller; the necessity by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject. |

| | | |
|---|---|---|
| Morocco | Decree No. 2-15-712 on the Protection of Sensitive Information Systems and Infrastructures of Vital Importance | **Category:** Local processing requirement<br>**Sector:** Critical infrastructure<br>**Description:** According to Art. 9 of Decree No. 2-15-712, companies and organisations operating in sectors of vital importance and using data deemed sensitive must host their infrastructure and digital databases on Moroccan territory. The concerned entities are defined as those that undertake activities related to the production or distribution of "goods and services essential to the satisfaction of the basic needs for the life of the populations or to the maintenance of the security capacities of the country". It is reported that a detailed list of sensitive infrastructure is kept secret by the government and its content reviewed at least once a year. |
| Morocco | Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data of February 23rd 2009 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 43 of the Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data, the transfer of personal data to a foreign country is only allowed if the country offers an adequate level of protection of the privacy and fundamental rights and freedoms of individuals. In the Decision No. 236-2015 of 18 December 2015, the Moroccan data protection authority (CNDP) recognised the following countries as offering an adequate level of data protection: Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.<br>The transfer of personal data to a country that does not provide an adequate level of data protection is only allowed subject to the certain conditions including the express consent of the data subject or if the transfer is necessary to safeguard the data subject's life, to safeguard the public interest, to comply with judicial obligations, for the performance of a contract between the controller and the data subject or pre-contractual measures taken at the request of the latter. Personal data may also be transferred if the transfer is carried out pursuant to a bilateral or multilateral agreement to which Morocco is a party, or with the express and reasoned authorization of the CNDP when the personal data processing guarantees a sufficient level of protection of privacy and of the fundamental rights and freedoms of individuals, in particular, because of the contractual clauses or internal rules to which it is subject. |
| Mozambique | Decree No. 66/2019 of 01 of August - Telecommunications Network Security Regulation | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** According to Art. 7 of the Telecommunications Network Security Regulation, personal data of the residents in Mozambican territory must be stored within the boundaries of national borders and governed by the jurisdiction of Mozambique. However, the network and public telecommunications service operator can store consumer data in the cloud, outside of the territorial space, provided it ensures that the personal data storage is subject to the national jurisdiction and it is made available to the authorities upon request. |
| Myanmar | Electronic Transactions Law (The State Peace and Development Council Law No. 5/2004)<br><br>Law Amending the Electronic Transactions Law (State Administrative Council Law No. 7/2021) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 27-A(ii) of the Electronic Transactions Law, as amended in 2021 by Law No. 7/2021, mandates the personal data administrator to seek the consent of the owner of data before any data transfer. However, the Law does not further regulate the ways to seek the owner's consent. |
| Netherlands | Public Records Act | **Category:** Local storage requirement<br>**Sector:** Public sector<br>**Description:** Certain public records have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records. The government organisations regularly make a “selection list” which categorises the type of information that should be kept and for how long. Examples include reports on which ministries base their policies, building permits, and documentation of special events or disasters. After 20 years, the government organisations transfer such documents to the National Archives or to a local or regional archive service located in The Netherlands. |

| | | |
|---|---|---|
| New Zealand | Financial Markets Conduct Act 2013 | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** Since its enactment in 2013, Sections 215 and 216 of the Financial Markets Conduct Act 2013 has required issuers of financial products to keep a register of their regulated products in New Zealand. Furthermore, Sections 455 and 456 require reporting entities such as issuers of financial products, registered banks, building societies, and credit unions to keep certain accounting-related records in New Zealand.<br>Under Section 458 of the Financial Conduct Market Act 2013, accounting records, or copies of them, must be retained by the financial market conduct reporting entity for a period of at least 7 years after the later of (a) the date the records are made; and (b) the date of completion of the transaction to which the records relate.<br>Despite this local storage requirement, the Act allows reporting entities to keep accounting records outside New Zealand if specific documents are kept in New Zealand such as the financial statements of any reporting entity and registered scheme it manages and any document annexed to those financial statements that gives legally required information (Section 456). The Act does not otherwise prohibit cross-border data transfers. |
| New Zealand | Companies Act 1993<br><br>Financial Markets Conduct Act 2013 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Since its enactment in 1993 as amended in 1994, Section 189 of the Companies Act 1993 has required registered companies to store specified internal records at the company's registered office (which must be an address in New Zealand) or another place in New Zealand at least for seven years after giving notice to the Registrar of Companies. These records include: minutes of all meetings and resolutions of shareholders, minutes of all meetings and resolutions of directors and directors' committees, certificates given by directors under the Act, copies of all written communications to all shareholders or all holders of the same class of shares.<br>Furthermore, under the same provision, following records are subject to a minimum retention period of seven completed accounting periods of the company: copies of all financial statements and group financial statements required to be completed under the Act and accounting records.<br>Despite this local storage requirement, Section 456 of the Financial Markets Conduct Act allows reporting entities to keep accounting records outside New Zealand if specific documents are kept in New Zealand such as the financial statements of any reporting entity and registered scheme it manages and any document annexed to those financial statements that gives legally required information. The Act does not otherwise prohibit cross-border data transfers. |
| New Zealand | Customs and Excise Act 2018 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Since its enactment in 2018, Section 354 of the Customs and Excise Act 2018 has required businesses importing and exporting from New Zealand to keep specified records in New Zealand at least for seven years unless an exemption applies. However, the Act exempts companies from this requirement for certain records of companies importing or exporting if they apply to and are authorized by the Chief Executive of the New Zealand Customs Service to keep the prescribed records with a specific person outside New Zealand (Section 355).<br>Section 354 states that (1) Every specified person must: (a) keep at a specified place, or cause to be kept at a specified place, any prescribed records for the prescribed period; and (...); (2) The period prescribed for the purposes of subsection (1)(a) must not exceed 7 years; (3) (...) specified place means (a) a place in New Zealand; or (b) a place outside New Zealand if, (i) after making an application under section 355(1), the specified person is authorised to keep the prescribed records, or to cause the prescribed records to be kept, at that place; or (ii) after making an application under section 355(2), another person is authorised to keep the prescribed records for the specified person at that place. |

| | | |
|---|---|---|
| New Zealand | Goods and Services Tax Act 1985 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Since its enactment 1985, Section 75 of the Goods and Services Tax Act 1985 has required registered entities to keep and retain specified tax-related records at least for seven years in New Zealand unless an exemption applies so that the Commissioner of Inland Revenue may assess the entity's goods and services tax liability. Under Section 75(5), which was inserted in 1992, the Commissioner of Inland Revenue may require taxpayers to retain such data for an additional period of 3 year in cases of a further audit or investigation. Taxpayers are also exempt from the local storage requirement if authorized by the Commissioner as long as the Commissioner imposes reasonable conditions under Section 75(6)-(7). This requirement has been in place since its enactment in 1985.<br>Pursuant to this section, Revenue Alert 10/02, which was issued in 2010 by the Commissioner of Inland Revenue but does not reflect its final position, provides that "[t]taxpayers are responsible for ensuring they comply with their record keeping obligations. Therefore, taxpayers using a cloud computing service will need to be satisfied that all their business records will be [also] stored in data centres located in New Zealand." |
| New Zealand | Tax Administration Act 1994 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Since its enactment in 1994, Section 22(2) of the Tax Administration Act 1994 has required certain classes of taxpayers to keep and retain specified records related to their tax liability in New Zealand at least for seven years unless an exception applies, so that the Commissioner of Inland Revenue may assess the taxpayer's tax liability. Under Section 22(5), the Commissioner of Inland Revenue may extend three additional years for an additional audit or investigation. Taxpayers are exempt from the local storage requirements under Section 22(8)-(9) if authorized by the Commissioner of Inland Revenue. This requirement has been in place since its enactment in 1994.<br>Pursuant to this section, Revenue Alert 10/02, which was issued in 2010 by the Commissioner of Inland Revenue but does not reflect its final position, provides that "[t]taxpayers are responsible for ensuring they comply with their record keeping obligations. Therefore, taxpayers using a cloud computing service will need to be satisfied that all their business records will be [also] stored in data centres located in New Zealand." |
| New Zealand | Privacy Act 2020 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The new Privacy Act 2020 which entered into force in December 2020 creates a conditional flow regime. Information Privacy Principle 12 in Section 22 of the Act governs cross-border data transfer. A business or organization may only disclose personal information to another organization outside New Zealand if the receiving organization:<br>- is subject to the Privacy Act because they do business in New Zealand;<br>- is subject to privacy laws that provide comparable safeguards to the Privacy Act - or they agree to protect the information in such a way (e.g., by using model contract clauses), or<br>- is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.<br>If none of these conditions is satisfied, a business may only make a cross-border disclosure with the permission of the data subject.<br>This regime does not apply to an overseas organization to hold or process on the business's behalf (e.g., cloud service providers).<br>Still, despite the IPP 12, a business may make a cross-border disclosure in urgent circumstances where it is necessary to maintain public health or safety or for the maintenance of the law.<br>This regime does not affect or limit other New Zealand law that regulates the availability of personal information (Section 24). |

| | | |
|---|---|---|
| Nicaragua | Law No. 787- Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 14 of the Personal Data Protection Law, the assignment and transfer of personal data of any kind to countries or international organizations that do not provide adequate levels of security and protection is prohibited. Art. 14 further states that the transfer to foreign countries is allowed in certain circumstance, including international judicial collaboration, exchange of personal data in health matters, bank or stock transfers, agreed transfer within international treaties, or international cooperation between intelligence agencies, regarding crimes regulated in Law No. 735 for the prosecution of organized crime. |
| Niger | Law No. 2022-059 of 16 December 2022, relating to the protection of personal data<br><br>Law No. 2017-28 of 03 May 2017, relating to the protection of personal data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** According to Arts. 62 and 63 of the Law No. 2022-059, transfer of personal data outside the country is subject to authorization from the Haute Autorité de Protection des Données Personnelles (HAPDP or High Authority of Personal Data Protection). Apart from the condition of authorization from the HAPDP, there are other conditions to be fulfilled, including that transfer can only be conducted to a country that guarantees a sufficient level of security or, if that condition is not met, that some conditions are fulfilled such as the authorization by the owner of the data, the necessity of the transfer for health or juridical procedure, among others.<br>This law repealed Law No. 2017-28, Art. 24 of which provided that a cross-border transfer was also subject to authorisation by the data protection authority. |
| Nigeria | Guidelines on Point-of-Sale Card Acceptance Services of the Central Bank of Nigeria, 2011 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Pursuant to Section 4.4.8 of the Guidelines on Point-of-Sale Card Acceptance Services of the Central Bank of Nigeria, all domestic transactions in Nigeria, including but not limited to POS and ATM transactions, must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian issuers and acquirers. |
| Nigeria | Nigeria Data Protection Act, 2023<br><br>Nigeria Data Protection Regulation (NDPR), 2019<br><br>Nigeria Data Protection Regulation 2019: Implementation Framework | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Sections 41(1) and 43(1) of the Data Protection Act (DPA) provide that a data controller is allowed to transfer personal from Nigeria to another country as long as there is an adequate level of protection of personal data in such country or the data subject consented to the transfer after being informed of the risk and did not withdraw the consent, the transfer is necessary for the performance of a contract to which the data subject is a party, the transfer is for the data subject's benefit, necessary for a public interest, necessary for legal action, or protect the vital interest of the data subject or third party.<br>Prior to the DPA, the Nigerian Data Protection Regulation, 2019 (NDPR) was the go-to regulation on data protection. Although enforceable, it remains a subsidiary legislation, and there was no specific commission to oversee data protection. According to Section 2.11 of the NDPR, personal data transfers are permitted on condition that the destination country offers an adequate level of data protection. Determining the level of data protection is a prerogative of the National Information Technology Development Agency (NITDA) based on the Honourable Attorney General of the Federation's (HAGF) consideration of the foreign country's legal system, rule of law, respect for human rights and fundamental freedoms, as well as relevant general and sector-specific legislation in public security, defense, national security, and criminal law. The countries whose levels of personal data protection is considered adequate are provided in the whitelist in Annex C of the Implementation Framework of the Data Protection Regulation and includes 42 countries in addition to the EU Member States and all African countries who are signatories to the Malabo Convention 2014.<br>Where transfer to a jurisdiction outside the whitelist is being sought, the Data Controller shall ensure there is verifiable documentation to conduct the transfer under one or more of the exceptions stated in Art. 2.12 of the NDPR. These include the consent of the data subject and the necessity for the performance of the contract. |

| | | |
|---|---|---|
| Nigeria | Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), 2019 | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** In 2013, the National Information Technology Development Agency (NITDA) released guidelines on Nigerian content development in information and communications technology, subsequently amended in 2019. One of the requirements in Section 13.1 (2) is that "data and information management firms", both foreign and domestic, are required to store all data concerning Nigerian citizens in Nigeria. It is reported that these requirements raise costs for foreign businesses seeking to invest in the Nigerian market and create an intractable barrier to market entry for firms that distribute their data storage and processing globally. Further, such requirements prevent Nigerian businesses from taking advantage of cloud computing services supplied on a cross-border basis. |
| Nigeria | Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), 2019 | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Section 13.2 of the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) requires Ministries, Departments & Agencies (MDAs) to ensure that all sovereign data is hosted locally on servers within Nigeria. The MDAs should also promote as mandatory the presence of system logs and other computer data logging technologies to aid in the effective troubleshooting and forensic investigation of events in Government systems. |
| Nigeria | Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), 2019 | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Section 11.1 (4) and 12.1 (4) of the Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) requires telecommunication companies and network service companies to host all subscriber and consumer data within the country in line with existing legislation. |
| Norway | Bookkeeping Act (2004) | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** The Norwegian Bookkeeping Act (Section 13) establishes local storage requirements for accounting data. However, exemptions can be sought – and are regularly granted – if adequate storage facilities cannot be found in Norway. Under an exemption, companies may store their data offshore so long as it can still be accessed by the Norwegian Tax Administration if required. |
| Norway | Act on the processing of personal data (Personal Data Act) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** The Act on the processing of personal data (Personal Data Act) implements the General Data Protection Regulation (GDPR) of the European Union in Norway. In addition to companies established in the European Economic Area (EEA), the Regulation applies extraterritorially to companies offering goods or services to data subjects in the EEA and companies that monitor the behavior of EEA citizens (Art. 3).<br>The Regulation mandates that data is allowed to flow freely outside the European Economic Area (EEA) only in certain circumstances listed in Chapter 5 of the Regulation. The main conditions for such a transfer are the following: the recipient jurisdiction has an adequate level of data protection; the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); the data subject has given his/her consent explicitly; or, the transfer is necessary for the performance of a contract between the data subject and the controller.<br>The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection. In addition, the EU-US Data Privacy Framework acts as a self-certification system open to certain US companies for data protection compliance since July 2023. |

| | | |
|---|---|---|
| Oman | Royal Decree 6/2022 promulgating the Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 23 of the Personal Data Protection Law provides that the controller may transfer personal data outside the borders of the Sultanate of Oman, in accordance with the controls and procedures determined by the Executive Regulations. Further, the Law prohibits transferring personal data which has been processed in violation of its provisions or if the transfer would cause harm to the data subject. |
| Oman | Local data processing requirement | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** It is reported that the Telecommunications Regulatory Authority (TRA) requires service providers to house servers in Oman if they provide services in the country. However, no regulatory provision has been identified in this area. |
| Pakistan | Restriction on cross-border data transfers | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** It is reported that Pakistan prohibits data transfers to any country that it does not recognize, including: Israel, Taiwan, Somaliland, Nagorno, Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Additionally, data transfers to India must be justifiable by the transferor. |
| Pakistan | Prevention of Electronic Crimes Act, 2016 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 4 of the Prevention of Electronic Crimes Act prohibits the transfer of data without the authorisation of the data owner. |
| Panama | Law No. 81 on Personal Data Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 5 of Law No. 81, the transfer of personal data of a confidential, sensitive or restricted nature by the company responsible for the database or its custodian shall be permitted, provided that the company and/or its country of residence provide a level of protection comparable to that of Law No. 81; or if the transferring entity takes all necessary steps to ensure that the data will be protected in a manner consistent with the Law No. 81 through contracts, codes of conduct or applicable international standards. Art. 5 lists the following exemptions: when the data subject has given his/her consent; in the case of bank, money, stock market or securities transfers; when the transfer of the information is required by law or in order to comply with international treaties ratified by the Republic of Panama; and when the transfer is necessary for the conclusion or execution of a contract concluded or to be celebrated by the interested party or in their interest. |
| Panama | Resolution No. 52. Establishing guidelines for the location of databases operating under the concept of cloud computing or cloud services | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Resolution No. 52, issued by the Panamanian Authority for Government Innovation in September 2021, requires government entities with mission-critical or sensitive data in the cloud to transition such data to in-country storage facilities by end of December 2022. However, according to foreign companies and cloud service providers, the Resolution has not had a material impact on their operations in Panama and enforcement mechanisms have not been implemented. |

| | | |
|---|---|---|
| Peru | Personal Data Protection Law No. 29,733<br><br>Regulation of Law No. 29,733 Supreme Decree No. 003-2013-JUS | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 15 of the Peruvian Data Protection Law and Art. 19 of its Regulation N. 003-2013-JUS, personal data can be transferred to other countries whose data protection level is considered to be adequate. If the recipient country does not have an adequate level of protection, the data transmitter must guarantee that the processing of the personal data is made in accordance with the Peruvian legal framework. This provision is not applicable in the following cases:<br>- when the data subject has granted their consent to the transfer of their data under these conditions;<br>- the transmission of personal data is conducted within the framework of international judicial cooperation or the application of international trade in this regard;<br>- international cooperation among intelligence agencies;<br>- when the personal data is necessary for the execution of a contractual relationship with the data subject;<br>- when referring to banking and security transfers;<br>- when the transfer is made for the purposes of protecting, preventing, diagnosing, and providing medical treatment to the data subject. |
| Philippines | Bangko Sentral ng Pilipinas (BSP) Circular No. 899 - Amendments to the guidelines on outsourcing | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** According to the Circular No. 899, offshore outsourcing of bank's domestic operations is permitted only when the service provider operates in jurisdictions which uphold confidentiality. When the service provider is located in other countries, the bank should take into account and closely monitor, on continuing basis, government policies and other conditions in countries where the service provider is based during risk assessment process.<br>The Bangko Sentral ng Pilipinas (the Central Bank of Philippines) examiners shall be given access to the service provider and those relating to the outsourced domestic operations of the bank. Such access may be fulfilled by on-site examination through coordination with host authorities, if necessary. |
| Philippines | Data Privacy Act of 2012 (Republic Act No. 10173)<br><br>Implementing Rules and Regulations of the Data Privacy Act of 2012 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 21 of the Data Privacy Act and Section 50 of the Implementing Rules and Regulations impose responsibility on the controller to ensure the confidentiality, integrity, and accessibility of the personal information transferred. Controllers are required to use contractual or other means to ensure that the third-party entity to whom the personal information is to be transferred for processing provides a comparable level of protection as that of the Philippines. In addition, data transfers to third parties, including transfers to an affiliate or parent company, require the consent of the data subject. |
| Philippines | Data Privacy Act of 2012 (Republic Act No. 10173) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 13 of the Data Privacy Act provides that the processing of sensitive data and privileged information is prohibited, except in some cases including when data subjects have given their consent, the processing of the same is provided for by existing laws and regulations, the processing is necessary to protect the life and health of the data subject or another person, the processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, and the processing is necessary for purposes of medical treatment. |

| | | |
|---|---|---|
| Poland | Act on Gambling Games | **Category:** Local storage requirement<br>**Sector:** Gambling sector<br>**Description:** Under the Act on Gambling Games, Art. 15.d, online gambling providers have to store data related to the gambling activities and transactions within the EU or the European Economic Area and provide permanent remote access to tax authorities. |
| Poland | Telecommunications Act | **Category:** Local storage requirement<br>**Sector:** Telecom sector<br>**Description:** Under Arts. 180a-180c of the Telecommunications Act, telecommunications providers are required to store certain types of user data for 12 months, including user identity, date and time and the type of connection, in the territory of Poland. |
| Romania | Emergency Ordinance No. 77 of 24 June 2009 regarding the organization and exploitation of games of chance | **Category:** Local storage requirement<br>**Sector:** Gambling sector<br>**Description:** According to Art. 15 of Emergency Ordinance No. 77, in order to conduct remote gambling activities, the gaming server is required to have a registration system capable of identifying the gamers as well as a system which stores and transmits data to a backup server which is situated on Romanian territory. The gaming server has to be approved by the National Gambling Office (Oficiul National pentru Jocuri de Noroc, ONJN) and in compliance with the procedure established under the implementing rules of the Emergency Ordinance. In addition, the game server and the backup server must store all data including the registration and identification of players, the stakes placed and the winnings paid out, for a period of five years after the prescription deadline in relation to the repayment of public debts related to this data.<br>Furthermore, Art. 15 provides that the communications equipment, other than one of the suppliers of electronic communication services and networks defined in the Government Emergency Ordinance No. 111/2011, must record the geographical location of the IP addresses as well as identifying the date, time and the duration of a game session once they have registered as a participant in a game on the organiser's website. It is required that the data be stored for a period of a minimum of five years from the date of collection and processing. Moreover, such equipment, as well as the central location at which the organiser's central ICT system, is to be installed on Romanian territory or on the territory of another EU Member State or another State party to the Agreement on the European Economic Area or in the Swiss Confederation. |
| Russia | Federal Law of the Russian Federation of 27 June 2011 No. 161-FZ About national payment system | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 30.6.4 of Federal Law No. 161-FZ requires that foreign-based credit card companies transmit data for all transactions within Russia through state-owned operator: the National System of Payment Cards. It is reported that affect the possibility for financial supplied to use their processing facilities located outside of Russia. |

| | | |
|---|---|---|
| Russia | Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ About personal data<br><br>Russian Federation Code of Administrative Offences of 30 December 2001 No. 195-FZ | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 18(5) of Federal Law No. 152-FZ provides that during personal data collection, including through the Internet, the data operator shall ensure that databases located within the Russian Federation are used to record, systematise, accumulate, store, update, modify and retrieve personal data of Russian citizens. However, the requirements do not apply to companies that do not receive the data directly from either data subjects or such third parties, or inadvertently in the course of normal business activity. Moreover, provided that personal data when initially collected is placed in a primary database located and maintained in Russia, personal data contained in the database may then be transferred abroad and placed in other secondary databases, provided the requirements for data transfers are complied with. As a result, once personal data is collected, it shall be placed in the database located in Russia (i.e., the primary database) and all mentioned operations on the data should be carried out locally. Afterwards, the data can be transferred abroad for further processing (i.e., to the secondary database).<br>It is reported that since 2015, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) has been active in enforcing the above-mentioned measure. For instance, in November 2016 subject to the claim from Roskomnadzor the court in Moscow restricted access to the LinkedIn social network due to the breach of the measure. Further cases mostly included administrative fines which were issued also to major multinational companies, including Meta Platforms, Inc. (formerly Facebook, Inc.), Twitter, Inc. and later WhatsApp LLC, Google LLC, Airbnb, Inc., Apple, Inc., Twitch Interactive, Inc., United Parcel Service, Inc., Pinterest, Inc., Likeme Pte. Ltd., Ookla, LLC., Snap Inc., Match Group, LLC, Hotels.com, L.P., Spotify AB, and Zoom Video Communications, Inc. Some companies also faced repeated higher fines.<br>The Code of Administrative Offences establishes fines of up to RUB 6 million (approx. USD 64,620) for the first offence and up to RUB 18 million (approx. USD 193,860) for the subsequent offence. |
| Russia | Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ About personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 12 of the Federal Law No. 152-FZ prohibits the cross-border transfer of data to countries that do not provide an adequate protection of data subjects. However, cross-border transfers of personal data are permitted in the following circumstances: (i) approved by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) as providing adequate protection, which will include countries party to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); or (ii) in cases where such transfer is necessary to protect the life, health, or other vital interests of the data subject or other persons. Starting from 1 March 2023, operators have to notify any cross-border transfers of personal data before such transfers and, for transfers to countries which are not 'adequate', obtain permission from the Roskomnadzor for the transfer, with limited exceptions. |

| | | |
|---|---|---|
| Russia | Federal Law of the Russian Federation of 7 July 2003 No. 126-FZ About communication<br><br>Federal Law of the Russian Federation of 27 July 2006 No. 149-FZ About information, information technologies and on information protection | **Category:** Local storage requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 64 of Federal Law No. 126-FZ requires telecom operators, to store in the territory of the Russian Federation the following information:<br>- Information on the facts of reception, transmission, delivery and (or) processing of voice information, text messages, images, sounds, video or other messages of users of communication services - within three years from the moment of the end of such actions;<br>- Text messages of users of communication services, voice information, images, sounds, video or other messages of users of communication services - up to six months from the moment of termination of their reception, transmission, delivery and (or) processing.<br>In addition, Art. 10.1 of Law No. 149-FZ requires distributors of information, such as internet and telecom companies, messengers, email services, forums and other platforms that allow the exchange information on the internet, to store in the territory of the Russian Federation the following information:<br>- Information on the facts of reception, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages of internet users and information about these users for one year after the end of such actions;<br>- Text messages of internet users, voice information, images, sounds, video and other electronic messages of internet users up to six months from the end of their reception, transmission, delivery and/or processing. |
| Rwanda | Regulation No. 02/2018 of 24/01/2018 on Cybersecurity | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 3 of the Regulation on Cybersecurity states that "Any bank licensed by the Central Bank must maintain its primary data on the territory of the Republic of Rwanda." |
| Rwanda | Regulation No. 010/R/CRCSI/RURA/020 OF 29/05/2020 Governing Cybersecurity | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 15 of the Regulation Governing Cybersecurity states that "All networks, systems and applications of the licensee shall not be managed, hosted, remotely accessed or located outside of the Republic of Rwanda unless explicitly authorized by the Regulatory Authority." This requirement applies to all ICT infrastructure and services, which include "data, system, equipment, networks and applications" (Art. 2). |
| Rwanda | Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 48 of the Law relating to Protection of Personal Data and Privacy outlines a set of conditions required to be met by a data controller or data processor in order to transfer personal data outside Rwanda. These include:<br>- Authorization from the Supervisory Authority;<br>- Consent by the data subject;<br>- Performance of a contract;<br>- Public interest grounds;<br>- Defense claim;<br>- Protection of vital interests of data subject;<br>- Legitimate interests by the data controller;<br>- Performance on international instruments ratified by Rwanda.<br>Art. 50 clarifies the first condition stating that all personal data must be stored in Rwanda unless the company has a valid registration certificate authorising it to store personal data outside Rwanda, which is issued by the National Cyber Security Authority. |
| Rwanda | Ministerial Instruction No. 001/MINICT/2012 of 12/03/2012 related to the Procurement of Information, Communication and Technology goods and services by Rwanda Public Institutions | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Art. 17 of the Ministerial Instructions on ICT Procurement denotes that all Government IT systems and applications that provide critical Government data shall be hosted in the National Data Center (NDC). Similarly, Art. 18 of the Ministerial Instruction on ICT states that Government institutions that host applications in their own data centers shall obtain backup services from the NDC. |

| | | |
|---|---|---|
| Rwanda | Regulation No. 001/R/TD-ICS/ RURA/016 OF 06/05/2016 Governing Telecom Network Security in Rwanda | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 16 of the Regulation Governing Telecom Network Security of 2016 restricts telecommunication service providers from transferring, storing or processing subscribers information outside of the Republic of Rwanda.<br>In 2017, Rwanda's telecommunications regulator fined MTN Rwanda (a subsidiary of South Africa's MTN Group) USD 8.5 million (10% of its annual turnover) for failing to process Rwandan customer data in the country by transferring it to Uganda and for running its information technology services outside Rwanda. |
| Saint Lucia | Data Protection Act | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 45 of the Data Protection Act 2011, data shall not be transferred to a country or territory outside Saint Lucia unless the country or territory ensures an adequate level of data protection or the Commissioner has authorized the data controller to transfer the data abroad. Alternatively, personal data can be transferred abroad under certain exceptions, which are listed in Art. 45.2. These include cases in which: (i) the data subject has given consent to the transfer; (ii) the transfer is necessary to safeguard national security; (iii) the matter concerns public security; (iv) the transfer is made on such terms as may be approved by Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject. |
| Sao Tome and Principe | Law No. 03/2016 - Aims to Guarantee and Protect the Personal Data of Individuals | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 19 of Law No. 03/2016, cross border transfer of personal data is only permitted to countries considered to provide adequate levels of protection, as determined by the National Data Protection Agency (ANPDP). However, according to Art. 20, the transfer to a legal system that does not ensure an adequate level of protection may be carried out by notifying the ANPDP, or is permitted where the data subject has given his/her consent;<br>- the transfer is necessary for the performance of a contract between the data subject and the controller;<br>- the transfer is necessary for the performance of a contract entered into in the interest of the data subject between the controller and third party;<br>- the transfer is necessary or required by law for the protection of an important public interest, or for the declaration, exercise or defense of a right in legal proceedings<br>- the transfer is necessary to protect the vital interests of a data subject; or<br>- the transfer is made from a register which, according to the laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest provided conditions laid down in the law for consultation are fulfilled in each case.<br>In addition, the ANPDP may authorise a transfer or a set of transfers of personal data to a jurisdiction which does not ensure an adequate level of protection provided that the controller ensures adequate mechanisms to ensure the protection of privacy and the fundamental rights and freedoms of persons and of their performance, in particular by means of appropriate contractual clauses. |

| | | |
|---|---|---|
| Saudi Arabia | Cloud Computing Regulatory Framework | **Category:** Local processing requirement<br>**Sector:** Cloud-computing sector<br>**Description:** The Communication and Information Technology Commission (CITC), the telecommunications regulator in the Kingdom of Saudi Arabia (KSA), issued a revised version 3 of its Cloud Computing Regulatory Framework (CCRF v3), which came into effect on 18/04/1442 H (corresponding to 3 December 2020). The CCRF v3 replaces version 2 of the Cloud Computing Regulatory Framework (CCRF v2). This version clarifies the restrictions regarding transfers of KSA government generated customer content outside Saudi Arabia.<br>Art. 3.3.8 of the CCRF v3 states that cloud computing service providers (CSP) and cloud computing subscribers shall not transfer any Saudi Government data outside the Kingdom, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes), unless this is expressly allowed under the laws or regulations of the Kingdom. Art. 3.3.9 also adds that cloud computing subscribers may not transfer, store, or process shared content from Saudi government agencies' data to any public cloud computing system, community cloud computing system or hybrid cloud computing system belonging to a service provider within the Kingdom, unless the CSP is properly registered with CITC. |
| Saudi Arabia | Essential Cybersecurity Controls (ECC – 1: 2018)<br><br>Cloud Cybersecurity Controls (CCC – 1: 2020) | **Category:** Local processing requirement<br>**Sector:** Critical infrastructure<br>**Description:** The National Cybersecurity Authority (NCA) has developed and implemented the Essential Cybersecurity Controls (ECCs) with the objective to set the minimum cybersecurity requirements for information and technology assets in organisations. The ECCs apply to all government organisations in the Kingdom and its companies and entities (i.e. semi-government entities), as well as private-sector organisations owning, operating, or hosting Critical National Infrastructures (CNIs). Section 4.2.3.3 of the ECCs, which deals with cloud computing and hosting cybersecurity, mandates that an applicable organisation's information hosting and storage must be inside the Kingdom of Saudi Arabia. It is reported that the NCA strongly encourages all other organisations in the Kingdom to 'leverage these controls and implement best practices to improve and enhance their cybersecurity'.<br>On the other hand, the NCA issued its Cloud Cybersecurity Controls (CCC) which aim to enhance the reliability of cloud computing services by providing secure cloud computing services that help withstand various cyber threats. In particular, the NCA noted that the CCC applies to cloud service providers and cloud service tenants which constitute any government organisation in the Kingdom of Saudi Arabia inside or outside the Kingdom and its companies and entities, as well as private sector organisations owning, operating, or hosting CNIs that currently use or are planning to use any cloud service. The CCC framework requires operators to provide cloud computing services from within country, including all systems including storage, processing, monitoring, support, and disaster recovery centers (Sections 2-3-P-1-10 and 2-3-P-1-11). The requirement applies to all levels of data. |
| Saudi Arabia | Cyber Security Framework of Saudi Arabian Monetary Authority | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 3.4.3 of the Cyber Security Framework of Saudi Arabian Monetary Authority mandates that financial institutions should use cloud services located in Saudi Arabia. If the cloud services are outside Saudi Arabia, financial services should obtain explicit approval from the Saudi Arabian Monetary Authority. These applies to banks, insurance and/or reinsurance companies, financing companies, and credit bureaus operating in Saudi Arabia. |
| Saudi Arabia | Implementing Regulations of the Income Tax Law | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Art. 56 of the Implementing Regulations of the Income Tax Law requires that a taxpayer's books be kept in Saudi Arabia. |

| | | |
|---|---|---|
| Saudi Arabia | National Data Governance Interim Regulations | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Saudi Arabia's National Data Management Office published the National Data Governance Interim Regulations, which requires firms to store and process personal data within Saudi Arabia "in order to ensure preservation of the digital national sovereignty over such data." Data Controllers may only process or transfer personal data outside the Kingdom after obtaining written approval from the relevant regulatory authority (Art. 5.4.16). |
| Saudi Arabia | Royal Decree M/19 of 9/2/1443H on Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 29 of the Personal Data Protection Law generally prohibits data controllers from transferring personal data outside of Saudi Arabia or disclosing personal data to an entity outside of Saudi Arabia, except where:<br>- the transfer or disclosure will not adversely affect the national security or the vital interests of the Kingdom;<br>- sufficient guarantees are provided to safeguard the data transferred or disclosed and to protect the confidentiality of the same and that they meet the minimum criteria stipulated in the Regulation;<br>- the Personal Data is exported is limited to the minimum amount necessary;<br>- consent of the Data Authority has been obtained in respect of the transfer or disclosure concerned. |
| Saudi Arabia | Internet of Things (IoT) Regulatory Framework | **Category:** Local processing requirement<br>**Sector:** Other<br>**Description:** Art. 7 of the Internet of Things (IoT) Regulatory Framework requires all servers, devices, and network components providing an IoT service, and all data relating to the service must be located within Saudi Arabia. |
| Saudi Arabia | General Principles for Personal Data Protection in the Telecommunication, IT, and Postal Services | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 5.4 of the General Principles for Personal Data Protection in the Telecommunication, IT, and Postal Services requires that service providers of telecommunication, IT and postal services process customers' personal data within Saudi Arabia and prohibits them from processing customers' personal data out of Saudi Arabia without the authorization of Communication and Information Technology Commission (CITC). |
| Senegal | Law No. 2008-12 of 25 January 2008 Concerning the Personal Data Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Law No. 2008-12 lays down the principle that data may only be transferred to a third country if that country ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. The adequacy of the level of protection is assessed under Senegalese law (Art. 49 of the Personal Data Act). Conditions also apply to the local exporter who, under Arts. 50 and 51, may transfer data to a third country that does not guarantee a sufficient level of protection, subject to certain safeguards such as the consent of the data subject, the necessity of the transfer, etc. |

| | | |
|---|---|---|
| Senegal | Local processing requirement | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Senegal has recently set up a data centre in the city of Diamniadio and the President of the Republic has instructed the Government and all State structures to host the State's data and platforms in this infrastructure. |
| Seychelles | Financial Leasing Act, 2013 | **Category:** Local storage requirement<br>**Sector:** Financial sector<br>**Description:** According to Section 56(1) of the Financial Leasing Act, every financial leasing institution shall maintain in the Seychelles for a period of at least seven years certain records including: customer identification records, during and after termination of the customer relationship; transaction records showing, for each customer, at least on a daily basis, particulars of its transactions with or for the account of that customer, and the balance owing to or by that customer. According to Section 56 (2), every record shall be kept in written form or kept in digital format and it shall be the duty of the financial leasing institution to ensure that adequate data recovery systems and procedures are in place. |
| Seychelles | Data Protection Act, 2023 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 47 of the Data Protection Act provides that personal data shall not be transferred outside Seychelles unless the data processor in the recipient country or territory ensures a comparable level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. In addition, the Commission may authorise the transfer of personal data to another country provided that the recipient country is part of a cross border privacy rules system that ensures that: a) cross-border rules system standards are legally enforceable against the data controllers and data processors as part of the certification system; b) data controllers and data processors have implemented security measures using a risk-based approach proportional to the probability of the threat and severity of the harm, the confidential nature of the information processed and the number of data subjects affected. The Commission may prohibit the transfer of data under this section as may be necessary in the public interest. |

| | | |
|---|---|---|
| Seychelles | Data Protection Act, 2023 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 47 of the Data Protection Act provides that personal data shall not be transferred outside Seychelles unless the data processor in the recipient country or territory ensures a comparable level of protection for the rights and freedom, or with the authorization of the Commission. Additional restrictions apply to certain categories of data. Section 22 establishes that processing of personal data relating to race, ethnic origin, biometrics, genetics, political opinions, religious or philosophical beliefs or for the purpose of identifying a person's health or sex life is prohibited, but some exceptions apply including in case of consent of the data subject. In addition, under Section 24, processing of personal data relating to criminal convictions and offences or related security measures based on the principles for lawful processing under this Act shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of a data subject. Moreover, Section 47(3) provides that personal data of Seychellois citizens pertaining to minors shall only be processed and transferred subject to the following: there is a designated data controller accountable for cross-border data processing in Seychelles; the transfer is made between intra group schemes and the headquarters is located outside Seychelles; the data controller or data processor has informed the data subjects about the location of the data processing and all other relevant information as specified under Section 27; the transfer is necessary to protect vital interests of the data subject.<br>In addition, Section 23 states that no person shall process the personal data of a child below the age of 18 years unless consent is given by the child's parent or legal guardian. The data controller shall obtain consent from the parents or legal guardians or verify that consent has been given in the case of data obtained from third parties, taking into account available technology. |
| Sierra Leone | National Civil Registration Act 2016 (No. 14) | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Section 28(3) and 34(2) of the Civil Registration Act mandate that the civil register, which contains personal data of residents, be maintained and kept at the chiefdom, district and national level. Likewise, the personal registration file should be kept at the region, district or chiefdom of the individual. This is applicable to personal data stored in the Civil Register. |
| Sierra Leone | Telecommunications Subscribers Identification and Registration Management Regulations, 2020 | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Section 19(1-2) of the Telecommunications Subscribers Identification and Registration Management Regulation empowers the National Telecommunications Commission to establish and maintain a central electronic database of communications service subscribers, in which all subscribers' information shall be stored. The database shall be housed either within the Commission or in another location as may be determined by the Commission. As Section 22(3-4) provides that the transfer and utilisation of subscribers' data outside the country are subject to specific approvals, it is expected that the location of the central electronic database should be in the territory of the country. |
| Sierra Leone | Telecommunications Subscribers Identification and Registration Management Regulations, 2020 | **Category:** Conditional flow regime<br>**Sector:** Telecom sector<br>**Description:** According to Section 22 (3-4) of Telecommunications Subscribers Identification and Registration Management Regulation, the transfer and utilisation of subscribers' data outside the country are subject to the provision of justification for the data use, the approval of the Commission, and the assurances of the security and confidentiality of the data/information. |

| | | |
|---|---|---|
| Singapore | Personal Data Protection Act 2012<br><br>Personal Data Protection Regulations 2021 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Section 26(1) of the Personal Data Protection Act, organizations are prohibited from transferring personal data to a country or territory outside Singapore unless they comply with the requirements prescribed by the Act. Organizations must implement appropriate measures to verify and ensure that the recipient of the personal data, located in the foreign country or territory, is bound by legally enforceable obligations that provide a standard of protection comparable to that of the Personal Data Protection Act. Section 26(2) of the Act allows organizations to apply to the Personal Data Protection Commission for an exemption from any of the restrictions outlined in Section 26(1).<br>Furthermore, Part 3 of the Personal Data Protection Regulations specifies that if a recipient of personal data holds a specified certification, granted or recognized under the law of the country or territory to which the personal data is transferred, they are considered to be bound by legally enforceable obligations to ensure a standard of protection for the transferred personal data that is at least equivalent to the protection provided by the Personal Data Protection Act. The specified certifications include those recognized under the Asia Pacific Economic Cooperation (APEC) Privacy Recognition for Processors System, applicable when the recipient is a data intermediary, or the APEC Cross-Border Privacy Rules in other cases. Additionally, data transfers are permitted under the following conditions:<br>- The individual has given consent to the transfer of their data, having been provided a reasonable summary, in writing, of the extent to which their data will be protected by standards comparable to the Personal Data Protection Act;<br>- The transfer is necessary for the performance of a contract between the organization and the individual or for the purpose of entering into such a contract;<br>- The transfer is necessary for the conclusion or performance of a contract between the organization and a third party, which is entered into at the individual's request;<br>- The transfer is necessary for use or disclosure in certain situations where the consent of the individual is not required under the Personal Data Protection Act, such as use or disclosure necessary to respond to an emergency;<br>- The data are in transit;<br>- The data are publicly available in Singapore. |
| Somalia | Data Protection Act - Law No. 005 of 2023 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 30 of the Data Protection Act provides that a data controller may not transfer personal data to a country outside the country unless one of the following conditions is met:<br>- the personal data will be received solely in country/ies that provide an adequate level of protection;<br>- the recipient is an international organisation whose policies and administrative and technical measures afford an adequate level of protection;<br>- the recipient is subject to a law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measure that affords an adequate level of protection; or<br>- the transfer meets one of the several criteria in Art. 31, which include consent or that the processing is necessary for the entering into or performance of a contract with the data subject. |

| | | |
|---|---|---|
| South Africa | Tax Administration Act, 2011 (Act 28 of 2011)<br><br>Public Notice on Electronic Form of Record Keeping in terms of Section 30(1)(b) of the Tax Administration Act, 2011 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** Sections 29 and 30 of the Tax Administration Act provide for restrictions in relation to electronic business and tax records. Specifically, Section 30(1)(b) requires that the records, books of account, and documents referred to in Section 29, must be kept or retained by tax payers (or their agents) in the form, including electronic form, as may be prescribed by the Commissioner of the South African Revenue Service (SARS) in a public notice appeared in the Government Gazzette No. 787.<br>The Public Notice provides that the electronic records must be in an acceptable form that satisfies the standards contained in the Electronic Communications and Transactions, 2002 (Act 25 of 2002); the records must be easily accessible for inspection by SARS at all reasonable times, if required; and the records must be kept and maintained at a place physically located in South Africa, unless otherwise authorised by SARS. However, such authorisation will only be given if, among other things, SARS is satisfied that the records can be accessed from South Africa and that their foreign location will not impair accessibility of the records. |
| South Africa | The Protection of Personal Information Act, 2013 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** South Africa has implemented a conditional flow regime that takes inspiration from the European model. According to the Protection of Personal Information (POPI) Act 4 of 2013, Chapter 9, Art. 72, data can be transferred to third countries only when:<br>- the recipient is subject to a law, binding corporate rules or a binding agreement that: » upholds principles for reasonable processing of information that are substantially similar to the conditions contained in POPI; and » includes provisions that are substantially similar to those contained in POPI relating to the further transfer of personal information from the recipient to third parties who are in another country;<br>- the data subject consents to the transfer;<br>- the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; and/or<br>- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and: » it is not reasonably practicable to obtain the consent of the data subject to that transfer, and » if it were reasonably practicable to obtain such consent, the data subject would be likely to give it. |
| South Sudan | Banking Act, 2012 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Section 63(6) of the Banking Act states that "no bank shall move all or any part of their administration, operations, books or records outside South Sudan without prior written consent of the [central] Bank." Section 84(2) provides that financial ledgers and other financial records shall be kept in South Sudan for a period not less than 10 years. Section 84(6) relates to non-financial records, which must also be kept within South Sudan. |
| Spain | Law 40/2015 on the Legal Regime of the Public Sector | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Art. 46bis of Law 40/2015 provides that the information and communications systems for the collection, storage, processing and management of the electoral census, the municipal registers of inhabitants and other population registers, fiscal data related to own or assigned taxes and data on users of the national health system, as well as the corresponding processing of personal data, shall be located and provided within the territory of the European Union. The data may not be transferred to a third country or international organisation, with the exception of those that have been the object of an adequacy decision of the European Commission or when so required for compliance with the international obligations assumed by the Kingdom of Spain. |

| | | |
|---|---|---|
| Sri Lanka | Personal Data Protection Act, No. 9 of 2022 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 26 of the Personal Data Protection Act provides that a controller or processor other than a public authority may process personal data:<br>- in a third country prescribed pursuant to an adequacy decision;<br>- in a country, not being a third country prescribed pursuant to an adequacy decision, only where such controller or processor ensures compliance with the obligations imposed under Part I, Part II, and Sections 20, 21, 22, 23, 24, and 25 of Part III of Act No. 9; or<br>- in the absence of an adequacy decision mentioned in point one above or appropriate safeguards mentioned in point two above, a controller or processor other than a public authority may process personal data outside Sri Lanka in certain special instances listed in Section 26(5). |
| Sri Lanka | Personal Data Protection Act, No. 9 of 2022 | **Category:** Conditional flow regime<br>**Sector:** Public sector<br>**Description:** Section 26 of the Personal Data Protection Act provides that where a public authority processes personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Data Protection Authority, in consultation with the relevant controller or processor and the relevant regulatory or statutory body, classifies the categories of personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision.<br>Public authority is defined as a Ministry, any Department or Provincial Council, local authority, statutory body or any institution established by any written law, or a Ministry, any Department or other authority or institution established or created by a Provincial Council. |
| Sudan | Ban to transfer and local processing requirement | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** The laws do not mention the limitation to transfer data in a foreign country, but it is reported that de facto there is limitation to transfer data abroad for security reasons, especially for the strategic and sensitive sectors, such as telecom and audio-visual. |
| Sweden | Swedish Accounting Act | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to the Accounting Act (chapter 7 section 2§), documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years, and must be "immediately" made available to the Financial Services Authority for the purposes of market supervision. |

| | | |
|---|---|---|
| Taiwan | Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Art. 18 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (Regulations) deals with conditions upon which a financial institution may outsource its operations to overseas service providers. The financial institution must obtain a confirmation letter from the financial authority of the country where the outsourced services are conducted agreeing to the outsourcing operations. A foreign bank branch in Taiwan, on top of the confirmation letter, shall obtain the letter of consent authorized by its head office or regional head office to the obtainment and use on data, security control and cooperation with the supervisory requirements in Taiwan.<br>If the financial institution cannot obtain the letter of confirmation from the foreign financial authority, it must submit the following documents to the Financial Supervisory Commission:<br>- A letter of consent from the service provider, agreeing that where necessary, a person designated by the financial institution may examine the outsourced items. The aforesaid designated person may also be assigned by the competent authority at the expense of the financial institution;<br>- The evaluation on internal control principles and operating procedure of the service provider;<br>- The legal opinion indicates the protection of customer data where the service provider is located is not below the condition in Taiwan;<br>- The financial statements of service provider audited and attested by a CPA for the most recent fiscal year;<br>- A statement issued by the service provider certifying that no violation on customer interests, personnel malpractice, information and technology security and other occurrences that impact sound business operation in the last three years. |
| Taiwan | Personal Data Protection Act | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 21 of the Personal Data Protection Act (1995), the government may impose restrictions on a cross-border transfer of personal data by a non-government agency if (a) major national interests are involved, (b) an international treaty or agreement so stipulates, (c) the country receiving the data lacks proper regulations on protection of personal data and the data subjects' rights and interests may be consequently harmed, or (d) the transfer to a third country is carried out to circumvent the Act. |
| Taiwan | Restriction Order for communication business operators to transfer personal data of other users to the mainland | **Category:** Local processing requirement<br>**Sector:** Media sector<br>**Description:** In September 2012, the National Communications Commission issued the Restriction Order for communication business operators to transfer personal data of subscribers to the mainland China. The blanket order prohibits communications enterprises (i.e., telecom carriers and broadcasting operators) from transferring subscribers personal data to mainland China on the grounds that the personal data protection laws in mainland China are still inadequate. |
| Tajikistan | Data Protection Law - Act No. 1537 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 18.2 of the Personal Data Act, international transfers of data are permitted to countries that provide adequate protection for personal data. However, the law does not provide a definition or description of what constitutes 'adequate protection'. Moreover, cross-border transfers to countries that do not provide adequate protection are possible in the following cases: with the consent of the data subject; where provided by international treaties binding on Tajikistan; for the protection of the rights and freedoms of persons and citizens, if it is impossible to obtain consent; and where provided by law, if it is necessary for the protection of constitutional order, public order, the rights and freedoms of persons and citizens, the health and integrity of citizens, and state security. |

| | | |
|---|---|---|
| Tanzania | Payment Systems (Licensing and Approval) Regulations, 2015 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 42 of the Payment Systems Licensing and Approval Regulations requires a payment system provider to place its primary data center in relation to payment system services in Tanzania. |
| Tanzania | The Personal Data Protection Act 2022, Act No. 11 of 2022 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Sections 31 and 32 of the Personal Data Protection Act permit the transfer of personal data outside Tanzania only on the following circumstances: a) to a country with an adequate personal data protection legal system (i.e. essentially equivalent levels of protection to that within Tanzania) provided the recipient has proven (i) such transfer is necessary for important reasons of public interest or any other legitimate purpose or (ii) the importance of the transfer and there is no reason to assume that the subject's legitimate interests may be prejudiced by the transfer or processing in the recipient country. The data collector or processor must carry out a prior data protection impact assessment on the need to transfer personal data and ensure the recipient of the data only processes the relevant information in the data and for the purpose for which the data was transferred; b) to any other country with appropriate safeguards on the security and protection of personal data provided the data is transferred to be processed for a purpose approved by the data subject, unless the data subject has consented to such transfer, or the transfer is necessary:<br>- For the performance of a contract between the data subject and the data collector or the implementation of pre-contractual measures taken at the request of the data subject.<br>- For the conclusion or performance of a contract concluded or to be concluded in the interest of the data subject between the collector and another person.<br>- For any public interest or the establishment, exercise or defence of a legal claim.<br>- To protect the vital interests of the data subject.<br>- In accordance with a law aimed at giving information to the public which affords an opportunity for public consultation in general or anyone with a legitimate interest to submit their comments in accordance with a procedure laid down by law. |
| Thailand | Credit Information Business Act 2002 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** The Credit Information Business Act 2002 specifically covers the collection and processing of credit information. Chapter 2 states that only a credit information company has the right to operate the credit information business (section 9). Section 12 of the Act states that "No credit information company or information controller or information processor carrying on or operating the business in the Kingdom shall operate, control or process information outside the Kingdom." |
| Thailand | Personal Data Protection Act, B.E. 2562 (2019) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Part 3 of the Personal Data Protection Act 2019 (PDPA), transferring data outside Thailand is only allowed if the destination country has adequate data protection standards or approaches. There are four exceptions to the adequacy requirement in the law, as follows:<br>- A data subject's consent to transfer has been obtained;<br>- Specific statutory exemptions apply;<br>- The receiving organization provides suitable protection measures that enable the enforcement of data subject's rights;<br>- The receiving organization has put in place a "personal data protection policy" applicable to overseas data transfers.<br>According to Section 16(5) of the Act, the Personal Data Protection Committee (PDPC) has the power to announce and establish criteria for providing protection of personal data that is sent or transferred to a foreign country, including the list of adequate jurisdictions. |

| | | |
|---|---|---|
| Togo | Law No. 2019-014 Relating to the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Art. 28 of Law No. 2019-014 on the protection of personal data clearly states that data can only be transferred if the third country ensures an adequate level of privacy protection. Art. 29 admits a transfer of data provided that the transfer is one-off, not massive and that the person to whom the data relates has expressly consented to its transfer or if the transfer is necessary under specific conditions. Moreover, in Art. 30, the Data Protection Authority may authorize the transfer of data if the data controller provides sufficient guarantees with regard to the protection of privacy, fundamental rights and freedoms of the persons concerned and the exercise of the corresponding rights. |
| Togo | Law No. 2019-014 on the protection of personal data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** In accordance with Art. 21 of Law No. 2019-014, the processing of sensitive data is prohibited as a matter of principle. This includes all personal data relating to racial or ethnic origin, religious, philosophical, political or trade-union opinions or activities, sex life, health, social measures, prosecutions or criminal or administrative sanctions (Art. 4). However, this prohibition does not apply when, for example: the processing relates to data manifestly made public by the data subject; the data subject has given his or her consent in writing to such processing, in accordance with the texts in force; the data processing is necessary to safeguard the vital interests of the data subject or of another person in the event that the data subject is physically or legally incapable of giving consent; the processing is necessary for the establishment, exercise or defense of legal claims (Art. 22).<br>Processing is defined as any operation or set of operations provided for in Art. 2 of this law, whether or not carried out using automated processes, and applied to data, such as collection, exploitation, recording, organization, conservation, adaptation, modification, extraction, storage, copying, consultation, use, communication by transmission, dissemination or otherwise making available, alignment or combination, as well as the blocking, encryption, erasure or destruction of personal data (Art. 4). |
| Trinidad and Tobago | Data Protection Act | **Category:** Conditional flow regime<br>**Sector:** Public sector<br>**Description:** According to Art. 36 of the Data Protection Act, public entities must ensure or take steps to ensure that personal information in their custody or under their control is stored only in Trinidad and Tobago and accessed only in Trinidad and Tobago unless:<br>- The individual authorises their data to be exported;<br>- The information is stored in or accessed from another jurisdiction that has comparable safeguards as provided by the Data Protection Act. To this effect, the Office of the Information Commissioner is to publish a list of acceptable countries to transfer data to, which has not yet been published as Art. 36 is not yet in force and therefore is not binding as of this moment. |
| Tunisia | Decree-Law No. 2-2022, organizing the activity of credit information | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 21 of the Decree-Law No. 2-2022, it is forbidden for companies organizing the activity of credit information to transfer their databases outside Tunisia and to host the data in the cloud. |

| | | |
|---|---|---|
| Tunisia | Organic Act No. 2004-63 of 27 July 2004 on the Protection of Personal Data | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Pursuant to Organic Act No. 2004-63, the transfer of personal data is generally prohibited or subject to strict measures. According to Art. 52, prior authorisation from the Tunisian Data Protection Authority (Instance Nationale de Protection des Données à caractère Personnel, INPDP) is required in all circumstances. In addition, according to Art. 50, it is forbidden to transfer personal data to a foreign country where this is likely to harm the public security or vital interests of Tunisia. Lastly, according to Art. 51, the transfer of personal data is not permitted to countries which do not provide an adequate level of data protection. It should be noted that Art. 22 provides that the natural person or the legal representative of the legal entity wishing to carry out the processing of personal data and their agents must meet the following conditions: be of Tunisian nationality; be a resident of Tunisia; and have no criminal record. These conditions also apply to the subcontractor and its agents. |
| Tunisia | Ban on the transfer of personal data | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** It is reported that public companies and institutions are prohibited by the Ministry of Communication Technologies from freely transmitting and storing personal data outside of the country. |
| Türkiye | Payment Services and Electronic Money Institutions Law No. 6493 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** Art. 23 of Law No. 6493 requires that "the system operator, payment institution and electronic money institution shall be required to keep all the documents and records related to the matters within the scope of this Law for at least ten years within the country, in a secure and accessible manner". As a result, the information systems have to be located in the country. The article also specifies that "the information systems and their substitutes, which are used by system operator to carry out its activities shall also be kept within the country". |
| Türkiye | Banking Law No. 5411 | **Category:** Conditional flow regime<br>**Sector:** Financial sector<br>**Description:** Banking Law No. 5411 (only available in Turkish) foresees specific rules for cross-border transfers of customer data. Conditions regarding the cross-border transfer of customer data set forth under the Banking Law should take precedence over conditions set forth under the Data Protection Law. The Banking Law stipulates that even if the explicit consent of the customer is obtained pursuant to the Data Protection Law for cross-border transfers or transfers of customer data to third parties located in Turkey, the customer data should not be shared with and transferred to third parties located in Turkey or outside Turkey without the customers' instructions or requests (Art. 73).<br>Furthermore, under the Banking Law, the Banking Regulation and Supervision Authority is authorised to prohibit the sharing or transfer of customer data or bank secrets with third parties located outside Turkey, as well as to make decisions regarding keeping information systems used by banks and their backups locally due to evaluations regarding economic security. |

| | | |
|---|---|---|
| Türkiye | Law on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting - Law No. 5651<br><br>Social Network Provider Procedures and Principles (regulation of the Information and Communication Technologies Authority (ICTA) | **Category:** Local processing requirement<br>**Sector:** Media sector<br>**Description:** In July 2020, the Law on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting was amended. The amendments define the term "social network provider", oblige them to appoint a local representative, set out procedures for content removal, request reports every six months, and require user data to be stored within Turkey.<br>In September 2020, the Information and Communication Technologies Authority (ICTA) published a secondary regulation called "Social Network Provider Procedures and Principles", which clarifies the amendments applicable to social network providers. The amendments entered into force in October 2020.<br>Under the law, domestic or foreign social network providers that have more than one million daily accesses to their services from Turkey are obligated to store user data within the country (supplementary Art. 4). ICTA's secondary regulation (Art. 12) indicates that social network providers must prioritize storing users' basic information and the information required by ICTA within Turkey, and the measures must be reported every six months. |
| Türkiye | Personal Data Protection Law No. 6698 | **Category:** Conditional flow regime<br>**Sector:** Public sector<br>**Description:** According to Art. 9 of the Personal Data Protection Law, data cannot be processed or transferred abroad without the individual's explicit consent. Consent will not be required if the transfer is necessary to exercise a right or is required by law, and either:<br>- Sufficient protection exists in the transferee country, or<br>- if the data controller gives a written security undertaking and Turkey's Data Protection Board grants permission.<br>It is reported that these conditions are very restrictive, so that, in some cases, data controllers have made their own assessment of whether personal data will be adequately protected based on the criteria used by the Turkish Personal Data Protection Authority to assess adequacy. |
| Türkiye | Electronic Communications Law No. 5809 | **Category:** Conditional flow regime<br>**Sector:** Telecom sector<br>**Description:** Art. 51 of the Electronic Communications Law stipulates that the transfer of traffic and location data abroad is permitted with the data subjects' explicit consent. |
| Türkiye | Regulation on the Processing of Personal Data and the Protection of Confidentiality in the Electronic Communications Sector | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Art. 5.2 of the Regulation on the Processing of Personal Data and the Protection of Confidentiality in the Electronic Communications Sector prohibits the cross-border transfer of traffic and location data due to national security reasons. Traffic data is defined in Art. 4 as any data processed for communication or invoicing in an electronic communication network, for example, the parties in phone calls or the duration of the call, and location data is the specific data that determines the geographical location of the device belonging to the public electronic communication service user and processed in/through the electronic communication network. |

| | | |
|---|---|---|
| Türkiye | Decision No. 2018/DK-YED/27<br><br>Decision No. 2019/DK-TED/053 | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** According to Decision No. 2018/DK-YED/27, the emergency call (eCall) in vehicles, along with servers that provide the communication system allowing for value-added services, are to be located in Türkiye, and personal data in such systems cannot be transferred abroad without explicit consent. To achieve this, it is mandatory for the SIM cards, electronic SIMs (eSIMs) or modules having SIM card properties to be procured from operators licensed to provide mobile electronic communication in Türkiye or to be programmable to allow them to be controlled by such operators.<br>With Decision No. 2019/DK-TED/053, the localization requirements are no longer limited to eCall services only, encompassing all eSIM applications. Moreover, all infrastructure, system and storage units, including equipment and software related to the eSIM platform in GSMA standards, shall be established in Türkiye by a licensed local operator (or by a third party to be appointed by such local operators, but liability remaining with the local operator). The decision also states that all data should be kept within Turkish borders. Moreover, where the devices manufactured to be used in Türkiye or imported to the country have remotely programmable SIM (eUICC, eSIM/embedded SIM etc.) technologies, their relevant modules are expected to be programmable only by local mobile operators and only local mobile operator profiles may be installed. |
| Turkmenistan | Law of Turkmenistan No. 519-V About Information on Private Life and its Protection | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 17.2 of Law No. 519-V, the transborder transfer of personal data to the territory of foreign countries shall only take place if the protection of personal data is guaranteed by those countries. Furthermore, Art. 17.3. points out that the cross-border transfer of personal data to the territory of foreign countries that do not ensure the protection of personal data may be carried out in the following cases: 1) if the data subject has given his/her written consent to the cross-border transfer of his personal data; 2) if it is provided for by international agreements approved by Turkmenistan; 3) if provided by the laws of Turkmenistan, if it is necessary for the purposes of protecting the principles of constitutional structure, human and civil rights and freedoms, public health and morals, public order, protecting the country and ensuring state security; 4) to protect the life, health, other legal interests, constitutional rights and freedoms of the data subject or other persons, if it is not possible to obtain the data subject's consent. Otherwise, pursuant to Art. 17.4, the international transfer of personal data abroad may be prohibited or restricted by the legislation of Turkmenistan. |
| Uganda | National Payment Systems Act, 2020 - Act No. 15 of 2020 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** In accordance with Art. 68 of the National Payment Systems Act, all electronic money issuers are obliged to establish and maintain their primary data centre in relation to payment system services in Uganda. |
| Uganda | Obligation to establish a local data centre | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** In 2017, the Central Bank of Uganda reportedly interpreted the country's cybersecurity legislation as giving it the power to require financial institutions to relocate their data centres to Uganda in order to provide the government with access to customers' digital financial information. Regulated financial institutions are currently implementing this policy. |

| | | |
|---|---|---|
| Uganda | Data Protection and Privacy Act, 2019<br><br>Data Protection and Privacy Regulations, 2021 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 19 of the Data Protection and Privacy Act stipulates that in the event that a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller must ensure that the country in which the data is processed or stored has in place adequate measures for the protection of personal data at least equivalent to the protection provided for by this Act, or that the data subject has consented. In addition, Regulation 30 of the Data Protection and Privacy Regulations provides further details, including that any personal data processed outside Uganda shall not be further transferred to, or processed in, a third country without the express consent of the data subject. |
| UK | Companies Act 2006 | **Category:** Local storage requirement<br>**Sector:** Horizontal<br>**Description:** According to Section 388 of the Companies Act 2006, if accounting records are kept at a place outside the United Kingdom, accounts and returns must be sent to, and kept at, a place in the United Kingdom, and must at all times be open to such inspection. In addition, records must be sent back to the UK at intervals of not more than six months. |
| UK | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)<br><br>Data Protection Act 2018 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 44 of the United Kingdom General Data Protection Regulation (UK GDPR), it is required that any international data transfer of personal data to a third country or international organisation should only take place under certain conditions and/or with certain safeguards in place. These are further set out in Arts. 45 to 49 of the UK GDPR.<br>The 2018 Data Protection Act allows personal data to flow from the UK to third countries on the basis of an adequacy decision, appropriate safeguards (such as standard data protection clauses and binding corporate rules), or other conditions specified under the Data Protection Act. The UK has granted adequacy to countries within the European Economic Area, countries covered by European Commission adequacy decisions (as of 31 December 2020), and South Korea (as of 23 November 2022). |
| Uruguay | Law No. 18,331 - Personal Data Protection Law | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** According to Art. 23 of Law No. 18.331 - Personal Data Protection Law, the transfer of personal data to countries or international organizations that do not provide adequate levels of protection is prohibited. The prohibition shall not apply in the case of:<br>- International judicial cooperation, in accordance with the respective international instrument, whether Treaty or Convention, takes into account the case's circumstances;<br>- Exchange of medical data when so required by the affected person's treatment for public health or hygiene reasons;<br>- Banking or stock exchange transfers, in relation to the respective transactions and in accordance with the applicable legislation;<br>- Agreements within the framework of international treaties to which the Oriental Republic of Uruguay is a party;<br>- International cooperation between intelligence agencies in the fight against organized crime, terrorism fight against organized crime, terrorism, and drug trafficking. |
| US | Code of Federal Regulations<br><br>Federal Risk and Management Program Control Specific Contract Clauses | **Category:** Local processing requirement<br>**Sector:** Public sector<br>**Description:** Pursuant to the Code of Federal Regulations (§239.7602-2 of Part 239 of Chapter 2 of Title 48), cloud computing service providers to the U.S. Department of Defense (DoD) may be required to store data relating to the DoD within the US. The service provider's authorising official may authorise storage of such data outside of the US, but this will ultimately depend on the sensitivity of the data in question. Similarly, Section 2.1 of the Federal Risk and Management Program (FedRAMP) Control Specific Contract Clauses require agencies with 'specific data location requirements' to include contractual obligations identifying where 'data-at-rest […] shall be stored'. |

| | | |
|---|---|---|
| US | Network Security Agreements | **Category:** Local storage requirement<br>**Sector:** Telecom sector<br>**Description:** The United States has not adopted laws or regulations requiring that data be stored locally in the United States. Nevertheless, it is reported that in some cases Team Telecom - an informal grouping of the Departments of Defence, Homeland Security and Justice, and the Federal Bureau of Investigation - imposes requirements to store data locally in security agreements and assurances letters as a condition for the grant of a licence or consent for a merger or acquisition. In such cases, Team Telecom may require that such data be stored only in the United States, or that copies of such data be made available in the United States. |
| Uzbekistan | Law of the Republic of Uzbekistan on Personal Data - Act No. ЗРУ-547 | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Art. 27-1 of the Law on Personal Data provides that the owners and/or operators are obliged to ensure that databases containing personal data of citizens of Uzbekistan are collected, systematized, and stored using technical means physically located in the territory of Uzbekistan. Moreover, the operators have to register their databases in the State Register of Personal Databases. |
| Uzbekistan | Law of the Republic of Uzbekistan on Personal Data - Act No. ЗРУ-547 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** In accordance with Art. 15 of the Law on Personal Data, cross-border transfers of personal data can be carried out when a foreign state ensures adequate protection for the rights of the subjects of personal data. In the absence of such protection, the cross-border transfer of personal data is allowed in the following cases:<br>- the data subject has consented to the cross-border transfer of their personal data;<br>- there is a need to protect constitutional order, public order, the rights and freedoms of citizens, or the health and the morals of the population; or<br>- it is stipulated by international treaties.<br>The transfer of personal data may be prohibited or restricted in order to protect the constitutional system of the Republic of Uzbekistan, the rights and legitimate interests of citizens, or to ensure the security of the State. |
| Venezuela | Decree No. 1.402, enacting the Decree with Rank, Value and Force of Law on Banking Sector Institutions<br><br>Decree No. 8.079 with Rank, Value and Force of Law on Partial Reform of the Law on Banking Sector Institutions<br><br>Law on Banking Sector Institutions, Extraordinary Official Gazette No. 6.015 | **Category:** Local processing requirement<br>**Sector:** Financial sector<br>**Description:** According to Art. 97(8) of Decree No. 1402, banking institutions are prohibited from transferring their principal computer centres and databases, either in electronic form or as users' physical documents, to a foreign territory. The Superintendency of Banking Sector Institutions is in charge of issuing regulations to determine which computer centres and databases qualify as principal in accordance with a binding opinion issued by the Central Bank.<br>The repealed Banking Sector Institutions Law of 2010 contained a similar restriction in Art. 99 with the difference that it prohibited the transfer of all computer centres and databases and not only those determined to be principal. The 2010 law was reformed in 2011 by Decree 8.079, which maintained the restriction in Art. 99. This 2011 decree was repealed by Decree No. 1.402 of 2014. |
| Venezuela | Constitutional Chamber of the Supreme Tribunal of Justice's Decision No. 1,318 | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Based on the safety and confidentiality principle (No. 7) set forth in Decision No. 1318, the transfer of personal data to other countries requires the data owner's prior consent and that the recipient country has rules guaranteeing, at least, the same level of protection of personal data as Venezuelan regulations. |

| | | |
|---|---|---|
| Vietnam | Decree No. 13/2023/ND-CP on the Protection of Personal Data | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Under Art. 25 of the Decree No. 13/2023/ND-CP, any entity or individual that transfers personal data offshore within the scope of the Decree has to prepare, maintain, and file a Transfer Impact Assessment (TIA) with Department of Cybersecurity and Prevention of Cyber-Crimes under the Ministry of Public Security (MPS A05 Department) within 60 days after the transferor begins to process personal data. The offshore transfer of personal data is defined to be using the internet, digital means or digital equipment or other means to transfer personal data of Vietnamese nationals to a location outside of the territory of Vietnam or using a location outside of the territory of Vietnam to process personal data of Vietnamese nationals (Art. 2(14)).<br>The TIA must include, among other things:<br>- details of transferor and receiver(s); description and explanation of the purposes of the processing activities to be performed after such transfer;<br>- types of data to be transferred;<br>- assessment of the impact of the data processing activities;<br>- potential consequences, mitigation and/or prevention measures;<br>- consent of the data subjects with the mechanism for the data subjects to respond to or claim upon the occurrence of any incident; and<br>- a binding document between the transferor and the receiver of the personal data, outlining the rights and obligations and responsibilities of each party, etc (Art. 25(2)).<br>After the transfer is completed, the transferor must notify the MPS A05 Department (Art. 25(4)). |
| Vietnam | Decree No. 72/2013/ND-CP, amended by Decree No. 27/2018/ND-CP | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** Decree No. 72 establishes the management of Internet services and online networks. Arts. 22, 25, 28 and 34 require providers of websites, social networks, information on mobile network and online games, respectively, to have at least one server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies". In March 2018, the Vietnamese government issued Decree No. 27/2018/ND-CP to partially amend and enhance Decree No. 72. Requirements on local servers remain. |
| Vietnam | Decree No. 15/2020/ND-CP | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** In February 2020, the Vietnamese government issued Decree No. 15/2020/ND-CP to regulate administrative violations on post-telecommunications, radio frequency, IT and electronic transactions. Art. 44.1(d) of the Decree regulates penalties for not storing information at the server system with IP address in Vietnam for electronic newspapers, general websites or web portal and social networks subject to the license. Art. 95.3 regulates penalties for advertising email and internet message services using servers not located in Vietnam. |
| Vietnam | Law No. 24/2018/QH14 on Cybersecurity | **Category:** Local processing requirement<br>**Sector:** Telecom sector<br>**Description:** In June 2018, the Vietnamese government issued Law No. 24/2018/QH14 on Cybersecurity. Art. 26 requires that foreign providers of Internet services, telecom services and value-added services to open representative offices or branches in Vietnam. According to the Law, personal information of Vietnamese users or users within Vietnam must be stored domestically. In addition, Art. 25 of the Law states that Gateway Internet Connection operators are encouraged to establish in the territory of Vietnam. It is reported that the government will decide the duration for which such businesses must store users' data in the Vietnamese territory, but it is currently unclear which criteria will be used. The concept of "telecom services" and "Internet services" are not yet defined. |

| | | |
|---|---|---|
| Zambia | Cyber Security and Cyber Crimes Act, 2021 (No. 2 of 2021) | **Category:** Local processing requirement<br>**Sector:** Critical infrastructure<br>**Description:** Part V of the Cyber Security and Cyber Crimes Act is dedicated to the protection of critical information and critical information infrastructure, where the former is defined as any information that is declared critical by the Ministry on account of its importance to the protection of national security, economic, or social well being of Zambia, and the latter is any infrastructure that contains such information (Section 17). Section 18 of the Cyber Security and Cyber Crimes Act of 2021 has a local processing requirement for 'critical information', which is defined in Section 2 as 'information that is declared by the Minister to be critical for the purposes of national security or the economic and social wellbeing of the Republic'. All critical information must be stored on a server or data center within Zambia, unless otherwise authorised by the Ministry. |
| Zambia | Data Protection Act, 2021 (No. 3 of 2021) | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Section 71(1) of the Data Protection Act allows for the transfer of personal data outside Zambia, except sensitive personal data, on condition that:<br>- The data subject has consented; and the transfer is made subject to standard contracts or intra-group schemes that have been approved by the Data Protection Commissioner; or the Minister has prescribed that the transfer outside the Republic is permissible.<br>- The Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.<br>Consideration by the Minister to sanction the cross-border transfer of personal data is based on the adequate level of protection, having regard to the applicable laws and international agreements in the destination country; and that the enforcement of data protection laws by authorities with appropriate jurisdiction is effective (Section 71(2)). |
| Zambia | Data Protection Act, 2021 (No. 3 of 2021) | **Category:** Local processing requirement<br>**Sector:** Horizontal<br>**Description:** Section 70(3) states that "sensitive personal data shall be processed and stored in a server or data centre located in the Republic". Sensitive personal data is defined in Section 2 of the Act as personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms and includes: the race, marital status, ethnic origin, or sex of a data subject; genetic data and biometric data; child abuse data; a data subject's political opinions; a data subject's religious beliefs or other beliefs of a similar nature; whether a data subject is a member of a trade union; or a data subject's physical or mental health, or physical or mental condition. |
| Zimbabwe | Cyber and Data Protection Act [Chapter 12:07] | **Category:** Conditional flow regime<br>**Sector:** Horizontal<br>**Description:** Sections 28 and 29 of the Cyber and Data Protection Act establish a framework for the cross-border transfer of data. Data can be transferred to countries that offer adequate protection. In addition, data can be transferred if it is in the public interest to do so. The data subject must provide consent to their information being transferred. However, this consent may also be implied or offered ambiguously.<br>Moreover, Section 11 of the Cyber and Data Protection Act prohibits the processing of sensitive personal information unless with the consent of the data subject or where processing is for legitimate purposes. Sensitive data, according to Section 3 includes social, political, cultural information, as well as health and genetic information, and any information which may be considered as presenting a major risk to the rights of the data subject. |

## Authors

**Martina Francesca Ferracane**

Associate Professor, School of Computing, Engineering & Digital Technologies, Teesside University

Assistant Professor, Robert Schuman Center for Advanced Studies, European University Institute

martina.ferracane@eui.eu

**Simón González Ugarte**

Research Associate, Robert Schuman Center for Advanced Studies, European University Institute