Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 34 *XXXIV*
Number 4

Article 2

2024

Cross-Border Data Regulatory Frameworks: Opportunities, Challenges, and a Future- Forward Agenda

Andrew D. Mitchell

Neha Mishra

Cross-Border Data Regulatory Frameworks: Opportunities, Challenges, and a Future- Forward Agenda

Cover Page Footnote

* Professor, Associate Dean (Research), Faculty of Law, Monash University, Wellington Road, Clayton Victoria 3800, Australia; (andrew.mitchell@monash.edu). Declaration of Competing Interest: The authors received financial support from the DCO for this independent study. ** Assistant Professor, Geneva Graduate Institute, (neha.mishra@graduateinstitute.ch).

Cross-Border Data Regulatory Frameworks: Opportunities, Challenges, and a Future-Forward Agenda

Andrew D. Mitchell* & Neha Mishra**

This Article evaluates the existing regulatory framework for cross-border data flows across Bahrain, Djibouti, Jordan, Kuwait, Morocco, Nigeria, Oman, Pakistan, Rwanda, and Saudi Arabia. A common factor among these countries is that they are members of the Digital Cooperation Organization ("DCO"). It considers how these countries have devised laws, regulations, and policies on cross-border data flows to enable digital trade, and how these instruments promote the growth of a robust digital economy, both domestically and internationally. The Article then offers policy recommendations for DCO members to consider in developing relevant laws and regulations on data flows.

These recommendations focus on three main areas: facilitating data enablers, improving data safeguards, and minimizing data restrictions. In terms of facilitating data enablers, the Article recommends that DCO members engage in regional negotiations to create mechanisms for cross-border data flows for digital trade, update their regulatory frameworks to participate in existing mechanisms such as the Cross-Border Privacy Rules ("CBPR") mechanism, and actively consider participating in digital trade negotiations. For improving data safeguards, the Article recommends that DCO members implement and enforce data protection laws and regulations,

* Professor, Associate Dean (Research), Faculty of Law, Monash University, Wellington Road, Clayton Victoria 3800, Australia; (andrew.mitchell@monash.edu). Declaration of Competing Interest: The authors received financial support from the DCO for this independent study.

** Assistant Professor, Geneva Graduate Institute, (neha.mishra@graduateinstitute.ch).

consider joining the Global Privacy Assembly, and establish independent data protection authorities. In terms of minimizing data restrictions, the Article recommends that DCO members review and remove any existing data localization requirements, avoid enacting new data localization measures, and develop mechanisms for cross-border data transfers that are consistent with international standards.

INTRODUCTION

Cross-border data flows lie at the heart of the global digital economy and are a key driver of international trade.[1] Experts have qualified "data" as the fifth factor of production alongside the movement of goods, persons, services, capital, and data.[2] Emerging digital technologies underlying the Fourth Industrial Revolution, including Artificial Intelligence ("AI"), Internet of Things ("IoT"), blockchain, etc., are driven by the free movement of data across borders, enabling sophisticated application of Big Data analytics.[3] The movement of data across borders has also enabled the digitalization of knowledge sharing, greater digital connectivity, and new opportunities for economic growth and development.[4] Governments increasingly understand the importance of data as a strategic asset and are adopting various tools to achieve greater sovereignty over data and digital infrastructure.[5]

---

1 *See* James Manyika et al., *Digital Globalization: The New Era of Digital Flows*, MCKINSEY (Feb. 24, 2016), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows [https://perma.cc/2LX3-LGEB]; WORLD BANK GRP., HARNESSING THE POWER OF BIG DATA FOR TRADE AND COMPETITIVENESS POLICY 8 (2017); *Big Data for Sustainable Development*, UNITED NATIONS, https://www.un.org/en/global-issues/big-data-for-sustainable-development [https://perma.cc/YYN6-DG3D] (last visited Feb. 28, 2024).

2 *See* DAN CIUARIAK & MARIJA PTASKHINA, INT'L CTR. FOR TRADE & SUSTAINABLE DEV., THE DIGITAL TRANSFORMATION AND THE TRANSFORMATION OF INTERNATIONAL TRADE 1 (2018).

3 *See* WORLD ECON. F., A ROADMAP FOR CROSS-BORDER DATA FLOWS: FUTURE-PROOFING READINESS AND COOPERATION IN THE NEW DATA ECONOMY 3 (2020), https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf [https://perma.cc/E2RZ-MW49].

4 *See* JANE DRAKE-BROCKMAN ET AL., DIGITAL TRADE: TOP TRADE NEGOTIATION PRIORITIES FOR CROSS-BORDER DATA FLOWS AND ONLINE TRADE IN SERVICES 4 (2021), https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB04_LM04.pdf [https://perma.cc/G86L-MP2D].

5 *See* Anupam Chander & Haochen Sun, *Sovereignty 2.0*, GEO. L. FAC. PUBL'NS & OTHER WORKS 11–19 (2021), https://scholarship.law.georgetown.edu/facpub/2404 [https://perma.cc/35SH-9BNH] (describing how various governments are dealing with digital sovereignty).

Against this background, this Article examines the existing regulatory framework for cross-border data flows across members of the Digital Cooperation Organization ("DCO"): Kingdom of Saudi Arabia ("Saudi Arabia"), Republic of Rwanda ("Rwanda"), Islamic Republic of Pakistan ("Pakistan"), Sultanate of Oman ("Oman"), Nigeria, Kingdom of Bahrain ("Bahrain"), Kingdom of Morocco ("Morocco"), State of Kuwait ("Kuwait"), Hashemite Kingdom of Jordan ("Jordan"), and Republic of Djibouti ("Djibouti"). While the first nine DCO members either have an evolving or an established framework governing cross-border data flows, Djibouti (to the extent of our research) currently does not have any laws and regulations relevant to cross-border data flows.[6]

We have relied upon publicly available information in English in examining and mapping the regulatory frameworks across these countries. On certain occasions, where official translations of relevant laws, regulations, and policies were not made available to us, we have looked at unofficial translations, to the extent publicly available. We could not confirm the authenticity or accuracy of the unofficial translations.

The key objective of this Article is to evaluate how the DCO members have devised laws, regulations, and policies on cross-border data flows to enable digital trade and the extent to which these instruments promote the growth of a robust digital economy, both domestically and internationally. Based on this evaluation, this Article offers policy recommendations for DCO members to consider in the future development of relevant laws and regulations on data flows. The Article is solely focused on the regulation of cross-border data flows (as defined below in Part II). Broader aspects of domestic data/digital regulation including e-commerce laws, internet intermediary laws, national security laws, encryption, and online content regulation are outside the scope of this project. However, as and where necessary to understand the framework for cross-border data flows, this Article references related legal and policy instruments.

---

[6] *See e.g., Djibouti: Data Protection Factsheet*, DATA PROTECTION AFRICA, https://dataprotection.africa/djibouti [https://perma.cc/3UTf-AU8S] (last visited Mar. 30, 2024).

I. THE REGULATORY FRAMEWORK FOR CROSS-BORDER DATA FLOWS

Before evaluating the regulatory framework for cross-border data flows across various DCO members, we set out some key definitions and elements of the regulatory framework. In this Part, we first set out what constitutes cross-border data flows and how it is conducted through the open end-to-end architecture of the internet. Then, we assess three elements of the regulatory design for cross-border data flows: data enablers, data safeguards, and data restrictions. This Part sets out a three-fold policy design for powering digital growth and integrating with the global digital economy optimally: facilitate data enablers, improve data safeguards, and minimize data restrictions.

A. Key Concepts in Cross-Border Data Flows

Data flows through the internet are seamless and inherently cross-border in nature. In this Article, the term "cross-border data flows" refers to the movement or transfer of data across the globally distributed and decentralized network of the internet. In other words, all data (irrespective of its nature) flowing across servers based in different geographical locations and indifferent to territorial boundaries is encapsulated within the concept of cross-border data flows. "Data" itself refers to any digitally encoded information (i.e., coded and stored in zeros and ones; bits and bytes). Further, raw data can be distinguished from *information*, which refers to the meaning that data conveys when organized systematically, for instance, during Big Data processing. Nonetheless, most regulatory frameworks worldwide do not make a meaningful distinction between "data" and "information."

To understand the regulation of cross-border data flows, one must understand the internet's underlying architecture. The internet is a globally distributed network based on end-to-end architecture, wherein the network acts as a conduit to carry data from one node to another, irrespective of the content of the data and territorial

boundaries and based on technical protocols.[7] This globally distributed architecture creates opportunities for economic and technological efficiencies. For example, companies storing data across global servers benefit from economies of scale, better protection against data losses and hacking, and ensuring timely access to data such as by using edge caches.[8]

Governments may restrict cross-border data flows for various reasons, including ensuring compliance with domestic data protection laws, for national security reasons, to enable growth of the domestic sector, to safeguard against cyber threats, and so on. One of the most common regulatory tools to restrict cross-border data flows is data localization.[9] While there is no universal consensus on the definition, data localization can be broadly understood as any legal, regulatory, or policy measure requiring data to be collected, stored, processed, and routed locally, whether directly or indirectly.[10] Data localization measures remain controversial, with several experts arguing that they "can reduce resilience and performance of internet networks (which were not built to align with territorial boundaries), affect the integrity of underlying protocols (e.g., for data routing and transfer) and impede the inherent openness and universal accessibility of the internet."[11] Some even argue that data localization can be

---

7 *See* Simson Garfinkel, *The End of End-To-End?*, MIT TECH. REV. (July 1, 2003), https://www.technologyreview.com/2003/07/01/234174/the-end-of-end-to-end/ [https://perma.cc/49U7-LNJT].

8 *See* Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE (May 22, 2017), https://www.lawfaremedia.org/article/where-your-data-really-technical-case-against-data-localization [https://perma.cc/VUK2-G7ER].

9 *See* Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFO. TECH. & INNOVATION FOUND. (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ [https://perma.cc/DE2Y-EGMR].

10 *See* Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 WORLD TRADE REV. 341, 341 (2020), https://www.cambridge.org/core/journals/world-trade-review/article/abs/privacy-cybersecurity-and-gats-article-xiv-a-new-frontier-for-trade-and-internet-regulation/F46D255A399C0A30B9BA68021EC28947 [https://perma.cc/69Q4-LAHG].

11 U.N. Conference on Trade & Development, *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*, at 134, U.N. Doc. UNCTAD/DER/2021 (2021), https://unctad.org/system/files/official-document/der2021_en.pdf [https://perma.cc/A2CX-VCCV].

a source of internet fragmentation.[12] However, several governments have recently implemented data localization laws for varied policy reasons, as demonstrated below in Part II.

B. Regulatory Design for Cross-Border Data Flows for Digital Trade

In designing the domestic regulatory framework for cross-border data flows, governments need to consider various public policy interests, including cybersecurity, privacy, and data protection, as well as the domestic regulatory capacity, concerns of law enforcement and regulatory access to data, digital industrialization concerns, and domestic content regulation laws. In the Section below, we identify a tripartite framework to understand the regulation of cross-border data flows consisting of data enablers, data safeguards, and data restrictions. We then provide a regulatory design to optimize cross-border data flows for digital trade.

Several regulatory frameworks on cross-border data flows relate to personal data.[13] While different jurisdictions define personal data differently, it typically refers to any information that relates to an identified or identifiable living individual.[14] Some jurisdictions categorize some kinds of personal data as critical, sensitive, and important, and define it more precisely (see examples in Section II.C). In practice, the distinction between personal and non-personal data is not always clear, particularly with the advent of Big Data technologies.

1. Data Enablers

"Data enablers" refers to various policy and regulatory tools that enable cross-border data flows to facilitate cross-border digital

---

[12] *See Internet Way of Networking Use Case: Data Localization*, INTERNET SOC'Y (Sept. 30, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/ [https://perma.cc/8AM7-7NMK].

[13] U.N. Conference on Trade & Development, *G20 Members' Regulations of Cross-Border Data Flows*, at 9, U.N. Doc. UCTAD/DTL/ECDE/2023/1 (2023), https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf [https://perma.cc/27XJ-FDNT].

[14] *See, e.g.*, Council Regulation 2016/679, General Data Protection Regulation, art. 4(1), 2016 O.J. (L 119) 33; CAL. CIV. CODE § 1798.140(v) (Deering 2023).

trade. We include in this category both international and domestic legal and policy initiatives. For instance, when countries participate in regional frameworks that enable cross-border data flows, including by adopting common high-level norms on data protection, this can act as a data enabler. One such example is the Cross-Border Privacy Rules System ("CBPR") of the Asia-Pacific Economic Cooperation ("APEC").[15] Under the CBPR, privacy certification bodies (approved by the government) can issue certifications to companies that are compliant with the principles of the APEC Privacy Framework.[16] The APEC Privacy Framework, last updated in 2015, sets out core principles on data protection applicable to all "persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information."[17]

Similar solutions may be developed on a bilateral basis—for example, a bilateral agreement on cross-border data flows such as the EU-US Data Privacy Framework.[18] A similar mechanism can exist at a regional level—for example, the Association of Southeast Asian Nations ("ASEAN") has designed model contractual clauses for enabling cross-border data flows.[19] Other data enabler mechanisms include commitments in international trade agreements to prohibit data localization measures and enable cross-border data flows for electronic commerce (subject to certain public policy exceptions).[20]

---

[15] *See About CBPRs*, CROSS-BORDER PRIV. RULES SYS., https://cbprs.org/about-cbprs/ [https://perma.cc/43NQ-Z75B] (last visited Feb. 28, 2024).

[16] *See What Is the Cross-Border Privacy Rules System?*, ASIA-PACIFIC ECON. COOP., https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system [https://perma.cc/5FDL-B4EG] (June, 2023).

[17] ASIA-PACIFIC ECON. COOP., APEC PRIVACY FRAMEWORK (2015) 5 (2017), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) [https://perma.cc/LR5F-C977].

[18] *See generally* Commission Decision 2023/1795, 2023 O.J. (C 4745) 1, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj [https://perma.cc/BR9M-CZQN].

[19] *See generally* Ass'n of Se. Asian Nations, *ASEAN Model Contractual Clauses for Cross-Border Data Flows* (2021), https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf [https://perma.cc/A6MA-RX8M].

[20] *See* Mira Burri, *Data Flows and Global Trade Law*, *in* BIG DATA AND GLOBAL TRADE LAW 11, 24–28 (Mira Burri ed., 2021), https://www.cambridge.org/core/services/aop-

In addition to international initiatives, data enablers can also exist in domestic laws and regulations. For instance, several countries worldwide are now developing frameworks for open government data to enable meaningful and useful innovation using public datasets.[21] Many of these frameworks require that public data be open by default, transparent, and easily accessible in a user-friendly format.[22] Finally, provisions on data interoperability and data portability, which refer to the ability of the users to access their data across various devices and services, is also an important data enabler.[23] Other measures aimed at digital and data inclusion can also broadly fall within the scope of data enablers, such as measures that support small- and medium-sized enterprises ("SMEs") to digitize and adopt best-in-class data policies.

Governments must implement data enablers in their domestic laws and policies in a transparent, reasonable, and objective manner. Two key tools to achieve this in practice include independent supervisory authorities and a whole-of-government approach (especially given how data regulations are spread across different government departments and ministries).

2. Data Safeguards

As discussed above, governments often regulate cross-border data flows for legitimate public policy objectives.[24] Therefore, we introduce the second component in our framework, "data safeguards," which refers to the regulatory framework necessary to safeguard the various public policy interests in relation to data flows. A variety of domestic laws, regulations, and policies, applicable to the

---

cambridge-core/content/view/E98D121FC172A9F534DE9C310919E389/9781108843591c1_11-41.pdf/data-flows-and-global-trade-law.pdf [https://perma.cc/XJ9J-DT39] (describing the trends in international trade agreements in relation to data flows and data localisation).

21 *See* discussion *infra* Part II.

22 *See, e.g.*, Ministry of Youth & ICT, *National Data Revolution Policy*, at 7 (Apr. 2017) (Rwanda).

23 *See* Bennett Cyphers & Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, ELEC. FRONTIER FOUND. (Feb. 12, 2021), https://www.eff.org/wp/interoperability-and-privacy [https://perma.cc/CYK4-3UZT] (defining portability and interoperability).

24 *See* discussion *infra* Section I.B.

digital sector at large, can be relevant to cross-border data flows. We highlight some key examples below. We consider data safeguards as necessary regulatory preconditions to enable cross-border flows of data.

Several examples of data safeguards can be found in domestic data protection and privacy laws, wherein governments implement various rules to protect the rights of data subjects (i.e., the individual to whom the personally identifiable information pertains). Currently, 71% of countries in the world have adopted data protection laws.[25] The majority of these laws provide certain basic rights to data subjects to ensure that any personal data collected and processed about them is duly protected against unwanted surveillance and privacy breaches, as well as provide the user the ability to make informed choices regarding how their personal data is used by private and public entities.

Specific to cross-border data transfers and processing, several laws (discussed below in Part II) provide requirements for entities processing personal data, including informing the users about such transfers, getting their consent for transferring data abroad, and restricting cross-border data transfers to limited situations (such as those pursuant to legitimate contracts or with explicit governmental approval).[26] Several laws also restrict the cross-border transfer of personal data to only those jurisdictions deemed "adequate" or "safe" by using a whitelisting approach, wherein the relevant regulator identifies the list of jurisdictions where data transfer is permissible.[27]

In other scenarios, governments permit cross-border transfers of personal data, where the data controller (i.e., the entity that decides on the purpose and means of data processing) or data processor (i.e., the entity processing the data under the direction of the data controller) provide an undertaking or sign contracts (often government-approved model contracts) with third parties ensuring that any data

---

[25] *Data Protection and Privacy Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE & DEV., https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/TN74-7SW3] (last visited Feb. 27, 2024).

[26] *See* discussion *infra* Part III.

[27] *See* discussion *infra* Part III.

transferred and processed abroad is consistent with domestic law requirements.[28] Several of the above measures are intended to function as data safeguards. However, where such measures are not implemented objectively, proportionately, and transparently, they may create unnecessary barriers to data flows, as discussed below in Subsection 3.

Data safeguards can be found in several other domestic laws and regulations. For instance, domestic cybercrime laws prohibiting illegal access to data, such as hacking, constitute a data safeguard.[29] Similarly, online consumer protection laws may protect the interests of data subjects and thereby function as a data safeguard. Domestic cybersecurity laws and policies, which require companies and government entities to adopt international best practices and standards on cybersecurity, also qualify as data safeguards.[30] This is because protecting data and digital infrastructure from cybersecurity threats is an essential precondition to enabling data flows. Other mechanisms such as data classification schemes provide certainty regarding how rules apply to different categories of data and thus also act as data safeguards.[31]

For a measure to qualify as a data safeguard, it is important that it protects a legitimate public interest (for instance, protecting digital rights of digital trade consumers) and is implemented reasonably, objectively, and transparently. In other words, data safeguards should always act as preconditions to enable secure and trusted cross-border data flows.

---

[28] An example of a scenario where governments permit cross-border transfer of personal data under certain conditions is the European Union's General Data Protection Regulation (GDPR). Under the GDPR, personal data can be transferred outside the EU, but only if adequate protections are in place. One of the mechanisms to ensure these protections is through Standard Contractual Clauses (SCCs). *See* Council Regulation 2016/679, General Data Protection Regulation, art. 28, 2016 O.J. (L 119) 49–50.

[29] *See, e.g.*, Computer Misuse Act, 1993 § 3(1) (Sing.).

[30] *See, e.g.*, *Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [https://perma.cc/NE7N-8ZCZ] (last visited Feb. 5, 2024).

[31] *See, e.g.*, Nat'l Cyber Sec. Agency, *National Data Classification Policy*, 11 (2023) (Qatar).
https://assurance.ncsa.gov.qa/sites/default/files/publications/policy/2023/NCSA_CSGA_National_Data_Classification_Policy_EN_V3.0.pdf [https://perma.cc/FA77-ARC2].

3. Data Restrictions

The third prong of our framework consists of data restrictions, which refers to measures restricting cross-border data flows for digital trade, often leading to both technological and economic inefficiencies. These measures are often excessive and unrelated to the policy objective they seek to address. For instance, several kinds of cross-sectoral and sector-specific data localization measures fall within the scope of data restrictions when implemented disproportionately or excessively.[32] Another example of an overt data restriction is a potential or (arguably) unjustified ban on certain foreign digital or data-driven technologies.[33] An extreme form of data restriction would be a domestic legal or policy requirement that imposes specific routing requirements for data flows (for instance, if there is a requirement that all data must be routed only through the servers within the country, even if it is only for transit).[34] Therefore, in assessing data restrictions, policymakers must assess whether the data restriction is intrinsically linked to a domestic policy objective and if it is the least restrictive manner in which this policy objective can be practically realized.

4. Achieving the Regulatory Design in Practice

Achieving an optimal regulatory design for cross-border data flows is by no means straightforward. Countries may have different policy considerations depending on their state of economic development, political priorities, social and cultural values, and domestic regulatory capacity. To enable cross-border data flows for digital trade, taking into account these different policy considerations, we

---

[32] *See* discussion *infra* Part II.

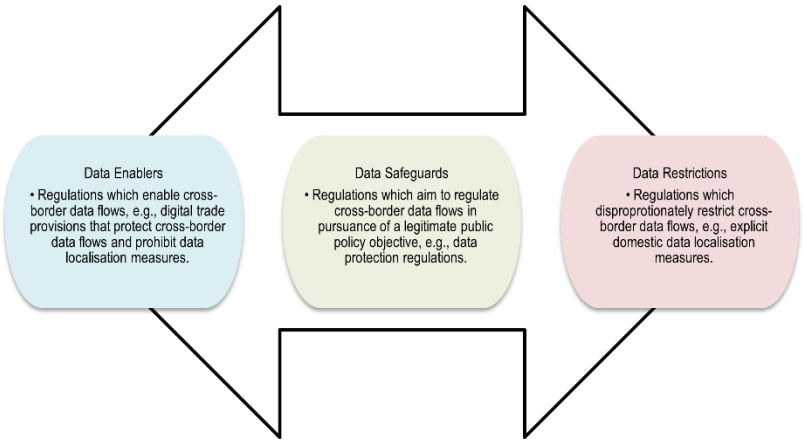
[33] *See e.g.*, Ben Lutkevich, *TikTok Bans Explained: Everything You Need to Know*, TECHTARGET (Dec. 1, 2023), https://www.techtarget.com/whatis/feature/TikTok-bans-explained-Everything-you-need-to-know [https://perma.cc/8BME-6VB6].

[34] *See, e.g.*, *Russia Internet: Law Introducing New Controls Comes into Force*, BBC (Nov. 1, 2019), https://www.bbc.com/news/world-europe-50259597 [https://perma.cc/N6ZE-Z92Q]; Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet*, GERMAN COUNCIL ON FOREIGN RELS.: ANALYSIS (Jan. 16, 2020), https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [https://perma.cc/B4RZ-W3AA].

propose a three-part framework: *Facilitate* Data Enablers, *Improve* Data Safeguards, and *Minimize* Data Restrictions. The application of this framework may vary in practice for different countries but provides a helpful baseline, as we explain in Part III. The proposed framework can be contextualized within each country's specific political and economic circumstances but must be implemented with transparency and good faith to the greatest extent possible. We underline the practical utility of this framework in Part III, where we provide detailed policy recommendations for DCO Members to consider in the near future.

Figure 1: Tri-partite conceptual framework

II. EVALUATING CROSS-BORDER DATA REGULATORY FRAMEWORKS FOR DCO MEMBERS



This Part highlights regulations across DCO Member countries to better understand the regulatory landscape for cross-border data flows. We provide a high-level country-by-country mapping of regulations relevant to cross-border data flows and highlight our key observations regarding the cross-border data regulatory framework. As qualified in the introduction, the examples discussed, and the inferences drawn in this Part are based only on publicly available information in English.

A. Saudi Arabia

Saudi Arabia has a highly complex and detailed framework for cross-border data flows, spread across various laws and policies. The government adopted a new data protection law on March 21, 2023.[35] The Saudi Data and Artificial Intelligence Authority ("SDAIA") acts as the supervisory authority for the Personal Data Protection Law ("PDPL").[36] Like most data protection laws, the PDPL applies to all entities (data controllers and processors) processing personal data for Saudi Arabian residents, irrespective of the entity's location.[37] Data subjects enjoy several rights including the right to be informed, access to personal data, correction of personal data, and deletion of personal data.[38] Further, data controllers and processors are bound by various obligations to inform data subjects about various aspects of data processing to obtain consent, implementing the principle of data minimization,[39] ensuring data security,[40] and implementing necessary measures to ensure that all cross-border transfers are compliant with domestic law.[41] However, where the controller is a government entity, the consent requirements are waived for security or judicial requirements.[42]

The PDPL contains a data localization requirement for all personal data, thereby restricting cross-border transfer of personal data, except when it is necessary to protect the data subject's life, their

---

35 *See generally* Saudi Data & AI Auth., Personal Data Protection Law (issued pursuant to Royal Decree No. M/19 of 9/2/1443 AH (corresponding to 16/09/2021 G), as amended by Royal Decree No. M/148 dated 5/9/1444 AH (corresponding to 27/03/2023)) (Saudi Arabia), https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf [https://perma.cc/UY7Y-UNJJ] [hereinafter Saudi Arabia – Personal Data Protection Law 2023].

36 *See Saudi Arabia: Summary*, ONETRUST DATAGUIDANCE, https://www.dataguidance.com/jurisdiction/saudi-arabia [https://perma.cc/E5HT-EBHT] (last visited Feb. 28, 2024).

37 *See Saudi Arabia – Personal Data Protection Law 2023*, *supra* note 35, art. 2.

38 *Id.* art. 4.

39 *Id.* art. 10.

40 Nat'l Data Mgmt. Off., National Data Governance Interim Regulations, § 5 (June 1, 2020) (Saudi Arabia), https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf [https://perma.cc/VPM8-SR5B] [hereinafter Interim Regulations].

41 *See Saudi Arabia – Personal Data Protection Law 2023*, *supra* note 35, arts. 5, 8.

42 *Id.* art. 6.

biological well-being, or to protect data subjects against diseases.[43] Further, any data that is transferred abroad must not, among other things, be contrary to national security interests and must be conducted with the permission of the SDAIA.[44] In providing such permission on a case-by-case basis, the SDAIA will consider whether the foreign jurisdiction sufficiently protects the personal data of its residents and assess whether the transfer involves sensitive data (in other words, all sensitive data must be localized in Saudi Arabia under all circumstances).[45]

The Draft Personal Data Protection Interim Regulations indicate that Saudi Arabia will be providing a list of countries that will be deemed adequate for the purposes of data transfers under PDPL.[46] Additionally, the government of Saudi Arabia has developed other interim regulations to inform the application of data-related laws, including data classification, data sharing, and open data.[47] Data is classified as "top secret," "secret," "confidential," and "public," depending on the extent to which it relates to the national interest, functioning of the national governance systems, and impact on the resources of the country.[48] Further, the Computing Services Provisioning Regulations or "CSPR" (applicable to any company wishing to obtain a license to provide cloud services in the country) provides for a classification of all subscriber data into (i) extremely confidential; (ii) confidential; (iii) restricted; (iv) public; and (v) non-

---

43 *Id.* art. 29.

44 *Id.*

45 Sensitive data is defined as "any personal data that indicates or includes a reference to a person's racial or ethnic origin; religious, intellectual or political beliefs; membership of civil associations or institutions; criminal and security data; biometric data; genetic data; credit data; health data; location data; and data that indicates that one or both of an individual's parents are unknown." *Id.* art. 1.

46 Saudi Data & AI Auth., Draft of the Executive Regulation of Personal Data Protection Law, art. 30 (2022) (Saudi Arabia), https://istitlaa.ncc.gov.sa/en/transportation/ndmo/pdpl/Documents/Draft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%209.pdf [https://perma.cc/NTV7-7P85].

47 *See generally, e.g.*, Nat'l Data Mgmt. Off., *supra* note 40 (consisting of the Personal Data Protection Interim Regulations ("DPIR"), Data Classification Interim Regulations ("DCIR"), the Data Sharing Interim Regulations ("DSIR"), the Freedom of Information Interim Regulations ("IIR"), and the Open Data Interim Regulations ("ODIR")).

48 *Id.* § 4.3.

government data.[49] The CSPR contains restrictions on the storage of government data (i.e., anything except non-government data) by cloud service providers not registered in Saudi Arabia and further prohibits the transfer of government data abroad.[50]

The National Data Governance Interim Regulations, covering different aspects of data regulation, acknowledge the importance of transparency, accountability, and data security, although it remains to be seen how the government will implement it in practice.[51] Most notably, the Open Data Interim Regulations provide high-level principles of openness by default, open format, accuracy and comprehensiveness of data, and open availability.[52]

Saudi Arabia has implemented data localization measures in other sector-specific laws and regulations. For instance, the Outsourcing Regulation for Insurance and Reinsurance Companies requires: (i) companies to get a no-objection certificate from any material processing abroad; and (ii) any entity regulated by SAMA needs prior approval for using foreign cloud services.[53] The Income Tax Bylaws require that all taxpayers' books must be kept in Saudi Arabia.[54] At the same time, the local Labor Law requires that certain

---

[49] Commc'ns, Space & Tech. Comm'n, Cloud Computing Services Provisioning Regulations, RS10, § 3-3-1 (Oct. 2023) (Saudi Arabia), https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf (last visited Apr. 1, 2024).

[50] *Id.* §§ 3-3-8, 3-3-9, 3-3-10.

[51] *Interim Regulations*, *supra* note 40, § 5.2.

[52] *Id.* § 8.2.

[53] Saudi Arabian Monetary Agency - Ins. Supervision Dep't, Outsourcing Regulation for Insurance and Reinsurance Companies and Insurance Service Providers, paras. 35, 42 (Nov. 17, 2012) (Saudi Arabia), https://ia.gov.sa/Documents/Rules/en/IIR_4600_Outsourcing_Regulation.pdf [https://perma.cc/UJ3B-YHUX].

[54] Gen. Auth. Zakat & Tax, Executive Regulations for the Income Tax System (issued pursuant to Ministerial Resolution No. (1535) of 11/6/1425 AH (as amended by Ministerial No. (2568) of 12/8/1440 AH), art. 56 (2019) (Saudi Arabia), https://zatca.gov.sa/ar/HelpCenter/guidelines/Documents/%D8%A7%D9%84%D9%84%D8%A7%D8%A6%D8%AD%D8%A9%20%D8%A7%D9%84%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A%D8%A9%20%D9%84%D9%86%D8%B8%D8%A7%D9%85%20%D8%B6%D8%B1%D9%8A%D8%A8%D8%A9%20%D8%A7%D9%84%D8%AF%D8%AE%D9%84.pdf [https://perma.cc/2EHB-5K2H].

records, statements, and files be maintained only in the workplace.[55] Any Internet of Things ("IoT") service providers in Saudi Arabia must obtain a local license and host their servers and data inside the country.[56] Saudi Arabia has implemented regulatory frameworks on cybercrime,[57] cybersecurity,[58] critical infrastructure,[59] and e-commerce,[60] although none of these laws and regulations contain specific requirements for cross-border data flows.

B. Rwanda

Rwanda is one of the front-runners in data regulation in Africa. Several extensive requirements for data localization in Rwanda were implemented to boost the domestic digital economy. A new data protection law came into force on October 15, 2021.[61] The law sets

---

[55] *Data Localization/Residency*, BAKER MCKENZIE (May 8, 2023), https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/emea/saudi-arabia/topics/data-localizationresidency [https://perma.cc/8KG8-MSPN].

[56] Commc'ns & Info. Tech. Comm'n, Internet of Things (IoT) Regulatory Framework, § 7 (Sept. 2019) (Saudi Arabia), https://cyrilla.org/api/files/1589445890652isqa70h2gxs.pdf [https://perma.cc/M6BY-KZUN].

[57] *See generally* Anti-Cyber Crime Law, 8 Rabi1 1428, Royal Decree No. M/17 8/3/1428 AH (Mar. 26, 2007) (Saudi Arabia), https://www.wipo.int/wipolex/en/text/498373 (last visited Apr. 1, 2024).

[58] *See generally* Commc'ns, Space & Tech. Comm'n, Cybersecurity Regulatory Framework (CRF) for Service Providers in the Information and Communications Technology Sector (June 2020) (Saudi Arabia), https://www.cst.gov.sa/en/RulesandSystems/CyberSecurity/Documents/CRF-en.pdf (last visited Apr. 1, 2024); Nat'l Cybersecurity Auth., *National Cybersecurity Strategy* (Dec. 2020) (Saudi Arabia), https://www.nca.gov.sa/national_cybersecurity_strategy-en.pdf [https://perma.cc/Q75W-MCMW].

[59] *See generally* Nat'l Cybersecurity Auth., *Critical Systems Cybersecurity Controls* (2019) (Saudi Arabia), https://nca.gov.sa/files/cscc-en.pdf [https://perma.cc/YX87-Z4Y4].

[60] *See generally* E-Commerce Law, Royal Decree No. M/126 (July 10, 2019) (Saudi Arabia), https://laws.boe.gov.sa/Files/Download/?attId=be4eef55-50be-44e3-b94d-adbb011b5736 (last visited Apr. 1, 2024); Ministry of Commc'ns & Info. Tech., *Digital Economy Policy in the Kingdom of Saudi Arabia* (2020) (Saudi Arabia), https://www.mcit.gov.sa/sites/default/files/digitaleconomypolicy_en.pdf (last visited Apr. 1, 2024).

[61] Law Relating to the Protection of Personal Data and Privacy, Law No. 058/2021 of 13/10/2021 (2021) (Rwanda); *see also Rwanda Passes New Law Protecting Personal Data*, MINISTRY OF ICT & INNOVATION, https://www.minict.gov.rw/news-detail/rwanda-passes-new-law-protecting-personal-data [https://perma.cc/2JBR-8G9X] (last visited Feb. 29, 2024).

out extensive requirements for data processing,[62] including mandatory compulsory registration of all data controllers and processors with the National Cybersecurity Authority ("NCA").[63] In fact, any company processing personal data of Rwandans must designate a local representative, even if its operations are entirely outside the country.[64] The law contains a de facto requirement to store all personal data in Rwanda,[65] unless the data controller or processor obtains a certificate from NCA.[66] Some other limited grounds exist for cross-border transfer of personal data, including upon explicit consent of the data subject, where the transfer is necessary for the performance of a contract between the data controller and third party, on the grounds of public interest or for legal proceedings, or pursuant to Rwanda's international legal obligations.[67]

Rwanda has implemented various other data restrictions, including explicit localization requirements across other laws and regulations. For instance, all government IT systems and applications processing, storing, and providing critical government data and information must be stored in the National Data Center.[68] Notably, this data center was hacked in 2020.[69] All information regarding the internet and telecommunications service subscribers can only be

---

62 Law Relating to the Protection of Personal Data and Privacy, Law No. 058/2021 of 13/10/2021, art. 16 (2021) (Rwanda), https://kifc.rw/wp-content/uploaads/2023/01/04.Law_relating_to_the_protection_of_personal_data_and_privacy.pdf (last visited Apr. 1, 2024) (requiring the maintenance of data processing logs); *id.* art. 17 (requiring a record be kept of all data recipients); *id.* art. 18 (requiring all information about personal data transfers to be provided to the data subject).

63 *Id.* art. 29.

64 *Id.* art. 39.

65 *Id.* art. 50.

66 *Id.*

67 *Id.* art. 48.

68 Ministerial Instructions Related to the Procurement of Information and Communications, Technology, Goods, and Services by Rwanda Public Institutions, Ministerial Instructions No. 001/MINICT/2012 of 12/03/2012, art. 17 (2012) (Rwanda), https://commons.laws.africa/akn/rw/act/min/2012/1/media/publication/rw-act-min-2012-1-publication-document.pdf [https://perma.cc/L4H4-BB5D].

69 *See* James Barton, *Hackers Shut Down Rwandan Government Data Centre*, DEVELOPING TELECOMS (Feb. 28, 2020), https://developingtelecoms.com/telecom-technology/data-centres-networks/9270-hackers-shut-down-rwandan-government-data-centre.html [https://perma.cc/4ZE3-YZF9].

stored and processed within the country.[70] In 2017, MTN Rwanda (a mobile telecommunications company) was fined by the local authorities for hosting some data in Uganda.[71] However, credit information of Rwandans may be transferred abroad with the express approval of the National Bank of Rwanda.[72] Similar restrictions exist for operations of licensed telecommunication service providers, who need explicit authorization from the Rwanda Utilities Regulatory Authority ("RURA") to manage, host, remotely access, or locate networks, systems, and applications outside Rwanda.[73]

Rwanda has developed an extensive enabling framework for digital and data regulation to boost the domestic data-driven economy,[74] including detailed cybersecurity regulations to ensure the confidentiality, integrity, and availability of networks and systems,[75] as well as e-commerce enabling frameworks.[76] At the

---

[70] Regulations Governing Telecom Network Security in Rwanda, Regulation No. 001/R/TD-ICS/RURA/016 of 06/05/2016, art. 16(e) (2016) (Rwanda), https://www.rura.rw/uploads/media/Regulations_Governing__Telecom_Network_Security.pdf [https://perma.cc/H5RG-XXPN].

[71] *See* Clement Uwiringiyimana, *Rwanda Regulator Fines MTN Rwanda $8.5 MLN over External IT Hub*, REUTERS (May 17, 2017), https://www.reuters.com/article/rwanda-telecoms-idUSL8N1IJ2IJ [https://perma.cc/VAP7-8UQW].

[72] Governing Credit Reporting System, Law No. 73/2018 of 31/08/2018, art. 46. (2018) (Rwanda), https://www.bnr.rw/fileadmin/user_upload/CREDIT_REPORTING_SYSTEM_LAW.pdf [https://perma.cc/YGB7-PE63].

[73] Cybersecurity, Regulation No. 010/R/CR-CSI/RURA/020 of 29/05/2020, art. 15 (2020) (Rwanda), https://rura.rw/fileadmin/Documents/ICT/Laws/Cybersecurity_Regulation_in_Rwanda.pdf [https://perma.cc/6DPP-H3PB].

[74] *For instance, under one law, the ICT regulator is tasked with two key objectives: (1) "adoption of the principle that regulation should be technology-neutral, and therefore a prohibition against granting unjustified advantage to any particular technology;" and (2) "creation of an open and competitive market." Governing Information and Communication Technologies, Law No. 24/2016 of 18/06/2016, art. 10 (2016) (Rwanda),* https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Laws/ICT_LAW.pdf *[https://perma.cc/Q4A3-4P67].*

[75] Cybersecurity, *supra* note 73, art. 1.

[76] *See, e.g.*, Ministry of ICT, *Smart Rwanda 2020 Master Plan: Towards a Knowledge Based Society*, 29 (Oct. 2015) (Rwanda), https://www.minict.gov.rw/fileadmin/user_uplodd/minict_user_upload/Documents/Policies/SMART_RWANDA_MASTERPLAN.pdf; Nat'l Bank of Rwanda, *Rwanda Payment System Strategy: Towards a Cashless Rwanda 2018–2024*, § 4.3.1 (2017) (Rwanda).

domestic level, the National Data Revolution Policy ("NDRP") sets out an ambitious framework to develop an innovative domestic data sector, including establishing standards and principles for data management; developing human capital in data science; addressing data privacy, security and sovereignty-related concerns; and building a domestic framework on data governance.[77]

The NDRP emphasizes the need to develop domestic data capabilities, including hosting services and maximizing the economic benefits of domestically generated data.[78] It also distinguishes sensitive and non-sensitive data and requires all non-sensitive data to be open by default.[79] Further, the policy acknowledges the need for regional and global collaboration in the data industry through a Global Open Data Charter.[80] In a similar fashion, the Rwanda Open Data Portal encourages open and freely accessible data portals for both public and private sector data.[81] The need for data interoperability and sharing is also recognized in other policy frameworks, such as the Draft Rwanda Fintech Strategy.[82]

Rwanda is also a party to the African Continental Free Trade Agreement or "AfCFTA" (where an e-commerce protocol is being developed) and the Malabo Convention (setting out high-level principles on data and privacy protection).[83] The Malabo Convention

---

77 Ministry of Youth & ICT, *National Data Revolution Policy*, iii (Apr. 2017) (Rwanda).

78 *Id.* at 3.

79 *Id.* at 7. "Open by default" in the context of Rwanda's National Data Revolution Policy (NDRP) refers to the principle that all non-sensitive data should be readily accessible and available to the public. *See id.*

80 *Id.* at 11.

81 *See* Victor Muvunyi, *A Rwandan Open Data Portal*, MINISTRY OF ICT & INNOVATION, https://www.minict.gov.rw/news-detail/a-rwandan-open-data-portal [https://perma.cc/RD7N-XZTU] (last visited Feb. 29, 2024).

82 Ministry of ICT & Innovation, *Rwanda Fintech Strategy 2022–27: Roadmap to Strategy Implementation*, 15–16 (2022) (Rwanda).

83 *See generally* African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, EX.CL/846(XXV), https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [https://perma.cc/VRE8-9AL4] [hereinafter Malabo Convention]; African Union, *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection*, https://au.int/sites/default/files/treaties/29560-sl-

provides for the development of a framework in the African Union, which would allow data transfers within the Union and prohibits data transfers outside of the Union to countries that do not provide an adequate level of protection to personal data.[84]

C. Pakistan

Pakistan is currently in the process of updating various domestic data-related laws, including the development of a domestic data protection law, Personal Data Protection Bill 2023.[85] This bill identifies three categories of data: personal, sensitive, and critical.[86] It sets out extensive obligations for data controllers, including maintaining detailed records of processing.[87] It also requires data controllers to obtain consent for each data processing operation that has a different purpose.[88] Data subjects are bestowed with several rights, including data access and data portability rights.[89] Limited exceptions exist for processing without a data subject's consent, including when the processing is necessary for the performance of a contract or legal obligation to which the data controller is subject, to protect the interests of the data subject or legitimate interests of the data controller, or when the processing is necessary for judicial proceedings.[90]

Data localization requirements are contained in Section 31(2) of the bill, which requires that all "Critical Personal Data shall only be processed in a server(s) or digital infrastructure located within the

---

AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf [https://perma.cc/27AG-46E9] (last visited Mar. 24, 2024) (displaying that Rwanda became one of the signatories in 2019).

84 *See* Malabo Convention, *supra* note 83, art. 14(6).

85 *See generally* Ministry of Info. Tech. & Telecomm., *Draft of the Personal Data Protection Bill, 2023* (2023) (Pak.), https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf (last visited Apr. 1, 2024).

86 *Id.*

87 Ministry of Info. Tech. & Telecomm., *Personal Data Protection Bill 2021, Consultation Draft*, § 11 (Pak.), https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft(1).pdf [https://perma.cc/VHX5-LJH9].

88 *Id.* § 5(1).

89 *Draft of the Personal Data Protection Bill, 2023*, *supra* note 85, at 20, 28.

90 *Id.* at 13.

territory of Pakistan."[91] Critical personal data has been defined as "such personal data retained by the public service provider – excluding data open to the public – as well as data identified by sector regulators and classified by the Commission as critical or any data related to international obligations."[92] Section 32.2 of the bill further states that the data protection authority shall devise a mechanism for sensitive personal data (in consultation with the government) if it relates to public order or security.[93] All other personal data can be transferred outside Pakistan provided one of the following conditions are met: equivalent protection; binding agreement; explicit consent of the data subject; and under any other conditions specified by the Commission.[94]

Data localization measures are also contained in other laws. For example, any company that falls within the scope of "significant social media companies" (which either has more than half a million users in Pakistan or have been notified by the authority) must comply with data localization laws set out in all domestic laws.[95]

Pakistan has implemented an extensive framework for the regulation of all forms of media, including digital media.[96] It has also adopted a detailed regulatory framework for cybercrimes, including fraud, forgery, disruption of digital infrastructure, cyber-terrorism, hurt to national interests, identity theft, hacking, digital defamation,

---

91 *Id.* at 29.

92 *Id.* at 7.

93 *Id.* at 29.

94 *Id.*

95 Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules (2021), 1343 S.R. & O. 1753, 1755, 1761–62 (Pak.).

96 *See generally, e.g.*, *id.*; The Telegraphs Act, No. 13 of 1885, PAK. CODE (1885) (Pak.), https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-bp8%3D-sg-jjjjjjjjjjjj [https://perma.cc/UPK7-PZUC]; Wireless Telegraphy Act, No. 17 of 1933, PAK. CODE (1933) (Pak.), https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-a5eY-sg-jjjjjjjjjjjj [https://perma.cc/J9H5-Z99W]; Electronic Media (Programmes and Advertisements) Code of Conduct (2015), S.R. & O. No.1(2)/2012-PEMRA-COC (Pak.), https://moib.gov.pk/MediaLaws/coc2015.pdf [https://perma.cc/46PF-WHWF]; Citizens Protection (Against Online Harm) Rules (2020), S.R. & O. No.(1)/2019 (Pak.), https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2C%202020.pdf [https://perma.cc/43EX-QE58].

etc.[97] In addition, Pakistan has developed a National e-Commerce Policy to enable the growth of the domestic e-commerce sector; this policy identifies the importance of data sovereignty and data localization to be strategic for the growth of the domestic digital economy.[98] Further, the National Cybersecurity Policy of 2021 sets out "data colonization" as a cybersecurity threat.[99] The Digital Pakistan Policy 2018 proposed various initiatives to build an ecosystem for e-commerce in Pakistan and integrate government databases to enable Big Data analytics.[100] The Pakistan Cloud First Policy sets out a clear schematic for data classification: open data, public data, restricted data, sensitive data, and secret data, with each data category subject to different security standards.[101]

D. Oman

Like several other members of the DCO, Oman is also in the process of revising its domestic laws and policies to make them

---

97 *See generally* Prevention of Electronic Crimes Act, No. 40 of 2016, THE GAZETTE OF PAKISTAN EXTRAORDINARY, Aug. 19, 2016, https://www.nr3c.gov.pk/peca16.pdf [https://perma.cc/F2CG-ZJ3L]; Prevention of Electronic Crime Investigation Rules (2018), 979 S.R. & O. 1895 (Pak.), https://www.nr3c.gov.pk/pecorules18.pdf [https://perma.cc/9E29-MXUU]; Ministry of Info. Tech. & Telecomm., *National Cyber Security Policy 2021* (July 2021) (Pak.), https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf [https://perma.cc/2SR2-3SJA] [hereinafter Pakistan – National Cyber Security Policy 2021].

98 *See* Gov't of Pak.: Com. Div., *e-Commerce Policy of Pakistan*, 6 (Oct. 2019) (Pak.), https://www.commerce.gov.pk/wp-content/uploads/2019/11/e-Commerce_Policy_of_Pakistan_Web.pdf [https://perma.cc/7KUQ-WG23] [hereinafter e-Commerce Policy of Pakistan].

99 *Pakistan – National Cyber Security Policy 2021*, *supra* note 97, § 1.3.3(ii). Data colonization, in the context of Pakistan's National Cyber Security Policy 2021, refers to the phenomenon where large, often foreign, corporations collect and control extensive amounts of data from a country. The concern is that this control can lead to dependencies and may influence or limit the sovereign decision-making capabilities of the nation. The policy aims to address and counteract such scenarios, ensuring that Pakistan maintains control over its data and cyberinfrastructure, thereby protecting its national interests and sovereignty in the digital realm. *See generally* e-Commerce Policy of Pakistan, *supra* note 98.

100 *See also* Ministry of Info. Tech. & Telecomm., *Pakistan Cloud First Policy*, 5 (Feb. 2022) (Pak.) (describing the country's aims to digitize public bodies and create cloud platforms to host government data).

101 *Id.* at 19.

better suited to the digital economy. Certain domestic laws and regulations contain clear data restrictions. For instance, companies offering Voice Over Internet Protocol Services such as Zoom, Teams, etc. must obtain a license and comply with the requirement to maintain and store users' personal data within the borders.[102] Some of these restrictions were relaxed during the pandemic to accommodate the need for digital communications.[103] Similarly, the Website and Data Hosting Policy states that all government data must be hosted, transacted, and processed within the country as a default.[104] Few exceptions may apply for transferring government data outside of the borders, such as with the approval of the Cabinet of Ministers or regulatory approval (when a private entity is involved).[105]

The data protection law in Oman went into force on February 13, 2023.[106] While the law broadly applies to the processing of personal data, there are certain exclusions for national security and public interest, which include execution of a State's administrative functions, protecting financial and/or economic interests of the country, investigation of criminal offences, and so on.[107] This law provides several rights to data subjects[108] and imposes various obligations on

---

[102] Telecomms. Regul. Auth., Decision No. (34/2012) On Issuing the Regulation on the Provision of Public Voice Telecommunications Service via Voice Over Internet Protocol (VOIP), art. 3 (2012) (Oman), https://www.tra.gov.om/pdf/551decisionno34-2012.pdf [https://perma.cc/LE3P-4RX7].

[103] *See* ITP Staff, *Oman Government Unblocks Some VoIP Services*, EDGE (Apr. 10, 2012, 9:53 AM), https://www.itp.net/news/588597-oman-government-unblocks-some-voip-services (last visited Apr. 1, 2024); Kabeer Yousef, *TRA Lifts Ban on VoIP Calls*, OBSERVER (Mar. 17, 2020, 11:32 PM), https://www.omanobserver.om/article/14684/Head%20stories/tra-lifts-ban-on-voip-calls [https://perma.cc/6M8S-WDUY].

[104] Sultanate of Oman Info. Tech. Auth. – Governance & Standards Div., *Website and Data Hosting Policy*, § 3.3(4) (2017) (Oman), https://www.moheri.gov.om/userupload/Policy/Website%20and%20Data%20Hosting%20Policy.pdf [https://perma.cc/R2GA-QFF9].

[105] *Id.*

[105] Ahmed Al Barwani et al., *New Omani Personal Data Protection Law Comes Into Force*, AL TAMIMI & CO. (Feb. 22, 2023), https://www.tamimi.com/news/new-omani-personal-data-protection-law-comes-into-force/ [https://perma.cc/AC8B-9MA9].

[107] Personal Data Protection Law, Royal Decree 6/2022, art. 3 (Feb. 9, 2022) (Oman), https://qanoon.om/p/2022/rd2022006/ [https://perma.cc/T9DC-2V5K] [hereinafter *Oman – Personal Data Protection Law*].

[108] *Id.* art. 11.

data collectors and processors.[109] This is comparable to various international frameworks discussed in this Article, including requiring the express consent of data subjects to process personal data (subject to limited exceptions).[110] To process genetic data, vital data, health data, ethnic origins, sexual life, political and religious opinions, criminal convictions, and related security measures, companies are required to obtain permission from the ICT Ministry.[111] This Ministry also exercises broad powers under the law to determine controls and safeguards for cross-border data transfer and may stop transfers abroad from harming public interests.[112] Under the data protection law, any transfer of personal data outside the borders of Oman must be consistent with the controls and procedures set out under regulations under the PDPL (although these are yet to be issued).[113] All cross-border data flows are also subject to the orders of the Cyber Defence Centre (as applicable to national security exceptions).[114]

Oman has also developed various laws and regulations relevant to the digital economy, including enabling electronic transactions,[115] prosecuting cybercrimes (to align domestic laws with the Budapest Convention on Cybercrimes),[116] and facilitating national e-payments systems (including setting out procedures for licensing of e-payment companies).[117] The government set up a Cyber Defense

---

109 *Id.* art. 15.

110 *See e.g.*, *id.*; *supra* notes 38–41 and accompanying text.

111 *Oman – Personal Data Protection Law*, *supra* note 107, art. 5.

112 *Id.* arts. 6, 8.

113 *Id.* art. 23.

114 *Id.*

115 Electronic Transactions Law, Royal Decree 69/2008, art. 2 (2008) (Oman), https://www.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/FID201141683941152/Electronic%20Transactions%20Law%20English.pdf [https://perma.cc/528J-G8CR].

116 Cyber Crime Law, Royal Decree 12/2011, art. 2 (2011) (Oman), https://www.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/FID20114117574666/Royal%20Decree%20No%20122011%20-%20Issuing%20the%20Cyber%20Crime%20Law.pdf [https://perma.cc/8APB-4AA5].

117 *See* Bd. of Governors of the Central Bank of Oman, Decision 1/2019 Issuing the Executive Regulation of the National Payment Systems Law (July 22, 2019) (Oman), https://decree.om/2019/bgcbo20190001/ [https://perma.cc/MSW3-UJ6F].

Center to protect national interests in cyberspace and supervise capacity development in cybersecurity.[118]

The government has initiated various policy initiatives to enable widespread digitalization and data-driven development, including the eGovernment Transformation Policy (2012),[119] ICT Policy Review and E-Commerce Strategy for Development of Oman (2019),[120] Artificial Intelligence Policy (2021),[121] Digital Oman (2030),[122] National Program for AI & Advanced Technologies (2020),[123] National Digital Economy Program (2021),[124] and Data and Information Security Classification Guidelines (2020).[125] In particular, the adoption of the Open Government Data Policy (2020) and National Open Data Initiative (2014) aimed to create a flourishing data-driven economy by encouraging the release of high-value

---

[118] *See* Establishing the Cyber Defence Centre and Promulgating Its System, Royal Decree 64/2020, arts. 1, 5 (June 10, 2020) (Oman).

[119] *See generally* Info. Tech. Auth., *eGovernment Transformation Policies* (2012) (Oman), https://www.moh.gov.om/documents/10181/667459/eGovernment+Transformation+Policies.pdf/de2933ea-0816-4120-b2b1-e3047320c6cf [https://perma.cc/G3RN-P9RZ].

[120] *See generally* ICT Policy Review and E-Commerce Strategy Development for Oman, UN ESCWA (Jan. 2019), https://andp.unescwa.org/plans/1460 [https://perma.cc/L33D-QF82].

[121] *See generally* Ministry of Transp., Commc'ns & Info. Tech., *AI Policy* (Oman), https://opendata.om/wp-content/uploads/2021/07/2021-06-AI-Policy.pdf [https://perma.cc/5H47-GMHT] (English version not available).

[122] *See generally* Chen Jianhan, *Enabling ICT Talents to Support Oman's Digitally Driven Future*, OMAN DAILY OBSERVER (July 8, 2022, 8:11 PM), https://www.omanobserver.om/article/1121972/business/economy/emabling-ict-talents-to-support-omns-digitally-driven-future [https://perma.cc/6HST-Z7LC].

[123] *See generally The National Program for AI and Advanced Technologies*, MINISTRY OF TRANSP., COMMC'NS & INFO. TECH. (Oman), https://www.mtcit.gov.om/ITAPortal/Pages/Page.aspx?NID=292589&PID=200683 [https://perma.cc/R6YS-MD6Z] (last visited Mar. 1, 2024).

[124] *See generally* Ministry of Transp., Commc'ns & Info. Tech., *National Digital Economy Program Summary (2021)* (Oman), https://www.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/202112284942713/National%20Digital%20Economy%20Program.pdf (last visited Apr. 1, 2024).

[125] *See generally Data and Information Systems Security Classification Mapping Guidelines*, MINISTRY OF TRANSP., COMMC'NS & INFO. TECH. (Oman), https://www.mtcit.gov.om/ITAPortal/Pages/Page.aspx?NID=2038&PID=7415&LID=301%20(English%20version%20not%20available) [https://perma.cc/4BQG-JPMQ] (last visited Mar. 1, 2024).

public datasets to the masses[126] based on the principles of openness (including a free worldwide license) and non-discrimination.[127]

Finally, Oman has committed to various initiatives at the regional level affecting the framework for the data-driven economy. For example, Oman has ratified the Arab Convention on Combating Information Technology Offences, which requires criminalization of various cybercrimes and provides legal procedures for enforcement of cybercrime laws, including cross-border access to data and tracking information.[128] It has also signed some Free Trade Agreements ("FTAs") with international partners (such as with Singapore and the United States);[129] however, these treaties do not contain specific provisions for cross-border data flows and data localization. As a member of the fifteen-country Arab Digital Economy Vision (2020), Oman has also committed to various objectives to actively digitize both the public and private sector and set up relevant regulatory frameworks for the digital economy.[130]

---

[126] Currently, all public data is classified into four levels: top secret, secret, restricted, and confidential, but proposals have been made to enable new categories of public government data. *See* Info. Tech. Auth., *Data and Information Systems: Security Classifications Mapping*, § 6 (2017) (Oman), https://cert.gov.om/files/laws/Data_and_Information_Systems_Security_Classification_Mapping_EN.pdf [https://perma.cc/M4S4-QHUC]; Info. Tech. Auth., *Oman eGoverment: Open Government Data Policy* (2020), https://www.moheri.gov.om/userupload/Policy/Government%20Open%20Data%20Policy.pdf [https://perma.cc/2D94-CZT4] [hereinafter *Oman – Open Government Data Policy*].

[127] Some categories of government data cannot be treated as open data, such as personal data. *See Oman – Open Government Data Policy*, *supra* note 126, at § 3.2.

[128] League of Arab States, *Arab Convention on Combating Information Technology Offences*, arts. 23, 40 (Dec. 21, 2010), https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf [https://perma.cc/CXF9-73YY].

[129] *See* Free Trade Agreement, U.S.-Oman, Jan. 19, 2006, available at http://www.ustr.gov/trade-agreements/free-trade-agreements/oman-fta/final-text [https://perma.cc/5RG9-GU8D]; *Gulf Cooperation Council-Singapore Free Trade Agreement Enters into Force*, SING. MINISTRY TRADE & INDUS. (Sept. 1, 2013), https://www.mti.gov.sg/Newsroom/Press-Releases/2013/09/GULF-COOPERATION-COUNCIL-SINGAPORE-FREE-TRADE-AGREEMENT-ENTERS-INTO-FORCE#:~:text=The%20Gulf%20Cooperation%20Council%20%E2%80%93%20Singapore,force%20today%2C%201%20September%202013 [https://perma.cc/2P7D-XUVG].

[130] *The National Program for Digital Economy*, OMANUNA, https://oman.om/en/national-program-for-the-digital-economy [https://perma.cc/JZX9-EMY8] (last visited Mar. 1, 2024).

E. Nigeria

Nigeria is one of the fastest-growing digital economies in Africa.[131] It has adopted a suite of laws and policies to enable the growth of the domestic digital and data economy, including adopting a Data Protection Regulation in 2019[132] and a new domestic data protection law called the Data Protection Act in 2023.[133] The Data Protection Regulation sets out the core objectives of safeguarding privacy, fostering safe conduct of transactions, preventing data manipulation, and ensuring the competitiveness of Nigerian businesses in international trade.[134]

Consistent with the majority of data protection laws across the world, the regulation sets out an extensive basis for protecting data subject rights. It contains various requirements such as the right to data portability, the right to access and deletion of data, and the right to be forgotten.[135] It also includes distinct requirements for obtaining specific, legitimate, and lawful consent for processing personal data (subject to limited exceptions).[136] Data controllers and processors are also subject to several obligations such as a duty of care to data subjects[137] and developing data security measures,[138] including a broadly worded obligation for all data processors/controllers to secure personal data "against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements."[139]

---

131 *See generally* World Bank Grp., *Nigeria Digital Economy Diagnostic Report*, 5 (2019), https://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf [https://perma.cc/DN5A-72BG].

132 *See generally* Nat'l Info. Tech. Dev. Agency, *Nigeria Data Protection Regulation 2019* (2019) (Nigeria), https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf [https://perma.cc/L9VX-69GS] [hereinafter Nigeria Data Protection Regulation 2019].

133 *See generally* Nigeria Data Protection Act, 2023 (Nigeria), https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf [https://perma.cc/JM8H-9HCD].

134 *Nigeria Data Protection Regulation 2019*, *supra* note 133, § 1.1.

135 *Id.* § 2.1.

136 *Id.*

137 *Id.* § 2.1(2).

138 *Id.* § 2.6.

139 *Id.* § 2.1(1)(d).

The requirement for cross-border transfers of personal data is subject to an adequacy framework, with permission to be provided by the Attorney General.[140] In deciding whether a country can be included in the whitelist, the Attorney General will consider the following factors: legal system of the foreign country, including respect for human rights, rule of law, public security rules, and data protection laws.[141] If transfers are to be made outside the countries included on the whitelist, one of the following exceptions must apply: explicit consent of the data subject, when it is necessary for the performance of a contract, for reasons of public interest or legal claims, or to protect the vital interests of the data subject.[142] The law further provides other reporting obligations for countries transferring data abroad, including how the personal data will be protected in the foreign country.[143] Annex C of the Implementing Guidelines for the regulation sets out a list of all whitelisted countries, including all countries of the African Union, EU and EEA areas, and China.[144] Interestingly, the law provides that where the rules are insufficient, the judicial bodies can consider rules in the Malabo Convention (to which Nigeria is a party) and the EU GDPR.[145]

The data protection framework has been updated by the Nigeria Data Protection Act 2023. The law applies to private and public entities collecting personal data[146] as well as any data subjects connected to Nigeria.[147] It also establishes an independent Data Protection Commission.[148] While the Act confirms the adequacy

---

140 *Id.* § 2.11.

141 *Id.* § 2.11(b).

142 *Id.* § 2.12.

143 *Id.* pt. 2.12(f).

144 Nat'l Info. Tech. Dev. Agency, *Nigeria Data Protection Regulation 2019: Implementation Framework*, 43–46 (2020) (Nigeria), https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf [https://perma.cc/CS9B-VSTR].

145 *Id.* at 29–30.

146 Nigeria Data Protection Act, 2023 No. 23 (2023) 110:119 O.G. A723 § 2 (Nigeria), https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf [htpps://perma.cc/Y2B7-NJDG]. *But see id.* A724 § 3(2) (listing several exceptions for government entities, including national security, public order, and public morals).

147 *Id.* A723 § 2(2)(a)–(b).

148 *Id.* A724–5 § 4, A726 § 7.

framework as a basis for the cross-border transfer of personal data, it also provides alternative safeguard mechanisms such as binding model contracts (similar to the Standard Contractual Clauses and Binding Corporate Rules of the GDPR).[149] Limited derogations are available from the adequacy or safeguard mechanism. For instance, derogation is possible if the data controller has explicit consent of the data subject or where other legitimate interests are involved, such as public interests or where certain vital interests of the data subject might be at stake.[150]

The Nigerian government has also developed various other regulations relevant to the digital and data-driven sectors, including data restrictions. For instance, all telecommunications companies are required to host all subscriber and consumer data within Nigeria.[151] Further, these companies must only peer their internet traffic[152] at an Internet Exchange Point in Nigeria.[153] All government data must also be hosted locally;[154] to host government or sovereign data outside Nigeria, the companies must have the express approval of the National Information Technology Development Agency.[155] The government can also specify the foreign jurisdiction in which such data may be stored.[156] Further, the Guidelines on Point of Sale Card Acceptance Services require that all domestic transactions in

---

149 *Id.* A743 § 41(1) (a).

150 *See id.* A744 § 43(1) (c).

151 Nat'l Info. Tech. Dev. Agency, *Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)*, § 11.1(4) (2019) (Nigeria), https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf [https://perma.cc/VS6R-Q9XR] [hereinafter Guidelines for Nigerian Content Development].

152 Internet peering is a process where two or more networks connect and exchange traffic directly, rather than through a third party. *See Explainer: What is Internet Peering*, INT. SOC'Y (June 19, 2020), https://www.internetsociety.org/resources/doc/2020/explainer-what-is-interet-peering. Peering internet traffic in Nigeria means that telecommunications companies in Nigeria are required to exchange their internet traffic locally within the country.

153 *Guidelines for Nigerian Content Development*, *supra* note 151, § 11.1(5).

154 *Id.* § 12.2(1).

155 *Id.* § 13.1(2).

156 *Id.* § 13.1(2)(I).

Nigeria be switched using the services of a local switch[157] and shall not under any circumstances be routed outside Nigeria for switching between Nigerian issuers and acquirers.[158]

The Nigerian government has enacted several laws and policies in recent years to provide an enabling regulatory infrastructure because of the importance of developing a domestic data-driven digital economy. For instance, in 2015, Nigeria adopted a law to address cybercrimes and ensure the security of critical national information infrastructure.[159] It also proposed a framework to enable standards for data interoperability.[160] It also discussed a bill on electronic transactions and consumer rights.[161] These initiatives are aligned with the broader goals set out in various policy frameworks related to the data and digital economy, including the National Digital Economy Policy and Strategy 2020–2030 (which was aimed at

---

[157] This refers to the processing of electronic payment transactions within the country. In the context of Point of Sale ("POS") and other electronic payment systems, "switching" is the process of transferring transaction information from the merchant's terminal (where the transaction is initiated) to the relevant financial institutions (like banks or card companies) for authorization and processing. *See What Is Payment Switch—Working, Architecture, Features, and Benefits*, LYRA BLOG (July 1, 2020), https://lyra.com/in/what-is-payment-switch [https://perma.cc/K4KD-U97T]. A "local switch" in this context would be a payment processing system that is located within Nigeria. This system would facilitate the electronic transfer of financial information and funds between the buyer and seller's banks.

[158] Cent. Bank of Nigeria, *Guidelines on Point of Sale (POS) Card Acceptance Services*, § 4.4.8 (2011) (Nigeria), https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf [https://perma.cc/WTH5-KNAP]. This means that for all domestic transactions in Nigeria—those where both the issuing and acquiring banks (i.e., the customer's bank and the merchant's bank) are Nigerian—the electronic data related to the transaction must be processed by a switch located within Nigeria rather than be routed through a switch or processing center located outside the country. *Id.*

[159] *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, § 1 (Nigeria), https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf* [https://perma.cc/HYT3-TXBR].

[160] Nat'l Info. Tech. Dev. Agency, *Data Interoperability Standards*, 11–12 (2016) (Nigeria), https://nesgroup.org/download_policy_drafts/Data%20Interoperability%20Standards%20%282016%29_1661783485.pdf [https://perma.cc/6EQU-S7MM] [hereinafter Nigeria – Data Interoperability Standards].

[161] *Electronic Transaction: Senate Prepares Legal Framework to Guide Deals*, NIGERIAN TRIB. (Feb. 27, 2020), https://tribuneonlineng.com/electronic-transaction-senate-prepares-legal-framework-to-guide-deals/ [https://perma.cc/687A-8ED2].

boosting the growth domestic digital sector and content)[162] and the Nigeria Cloud Computing Policy 2019 (aimed at increasing cloud services adoption by the public sector and SMEs).[163] The Cloud Computing Policy 2019 also sets out a data classification framework classifying data as having limited sensitivity/non-confidential data (available as Open Government Data), moderate sensitivity (routine government data), sensitive data (secret government data), and classified data (related to national security).[164] The National Cybersecurity Policy and Strategy 2021 also provides a foundation for linking cybersecurity to broader ideas of sovereignty, human security, and economic prosperity.[165]

Like Rwanda, Nigeria is also a member of the AfCFTA.[166] It is also a member of the Economic Community of West African States ("ECOWAS"),[167] which has adopted a supplementary act on data protection.[168] Under this treaty, personal data should only be transferred to states that have an adequate level of data protection.[169] Nigeria is also actively participating in the ongoing negotiations at the

---

[162] *See generally* Fed. Ministry of Commc'ns. & Digit. Econ., *National Digital Economy Policy and Strategy (2020-2030)* (2019) (Nigeria), https://www.nipost.gov.ng/Site_Downloads/National_Digital_Economy_Policy_and_Strategy.pdf [**https://perma.cc/A2AW-TJGZ**].

[163] *See generally* Nat'l Info. Tech. Dev. Agency, *Nigeria Cloud Computing Policy* (2019) (Nigeria), https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf [https://perma.cc/6YGW-YCCG] [hereinafter Nigeria Cloud Computing Policy 2019].

[164] *Nigeria Cloud Computing Policy 2019*, *supra* note 163, § 9.

[165] *See* Fed. Republic of Nigeria, *National Cybersecurity Policy and Strategy*, 10–11 (2021), https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf [https://perma.cc/ZT6N-X9CB].

[166] *See State Parties*, AFCFTA, https://au-afcfta.org/state-parties/ [https://perma.cc/B5RY-3GVU] (last visited Mar. 1, 2024).

[167] *Member States*, ECON. CMTY. OF W. AFRICAN STATES ("ECOWAS"), https://www.ecowas.int/member-states/ [https://perma.cc/77WR-NS5B] (last visited Mar. 1, 2024).

[168] *See generally* Econ. Cmty. of W. African States [ECOWAS], Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (Feb. 16, 2010), https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf [https://perma.cc/P3ZY-58DW**]**.

[169] *Id.* art. 36.

World Trade Organization ("WTO") on e-commerce under the joint initiative.[170]

F. Bahrain

Bahrain has a comprehensive and progressive regulatory framework on cross-border data aimed at maximizing data flows to enable the digital economy while also developing data safeguards and data enabling mechanisms across various domestic laws and policies. Shortly after the enactment of the GDPR in the EU, Bahrain issued its data protection law which came into force on August 1, 2019.[171] The law created a category of sensitive personal data which includes "any personal information revealing—directly or indirectly— . . . an individual's race, ethnical origin, political or philosophical opinions, religious beliefs, affiliation to union, personal criminal record, or any information in relation to his health or sexual status."[172] Like most advanced data protection laws, this law provides a framework for fair and lawful data processing and protecting various interests of data subjects, including a clear framework for obtaining consent for the processing of personal data[173] and granting several rights (but excluding the right to data portability).[174] Processing sensitive data is subject to certain additional requirements, especially when it entails automated data processing.[175]

---

[170] *See Joint Initiative on E-Commerce*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm [https://perma.cc/3A9L-PKRZ] (last visited Mar. 1, 2024).

[171] See generally *Personal Data Protection Law, Law No. (30) of 2018 (Bahr.), http://www.pdp.gov.bh/en/assets/pdf/regulations.pdf [https://perma.cc/B99F-DJMJ]*.

[172] Id. *art. 1*.

[173] *Id.* arts. 4, 5.

[174] *Id.* arts. 17–26 (enumerating the rights of the data subject, but not enumerating the right to data portability).

[175] *Id.* art. 15; *see also* Resolution No. (45) of 2022 (Bahr.), https://www.bahrain.bh/wps/portal/en/!ut/p/z1/tZLNcoIwFIVfhY1L5l6CELe2TovtjFotIt
k4AYKmShIxtT9PX3DXhWIXzSp35pxJzvkuMFgBU_wkN9xKrfi-
mVMWrr1xgNHgHjGazEYYTqMBJfTOn858SH4LvNcY8WU5Hs6nDyMP-
x6wW_x44QzxNv9FAenyL4EBM7ksIPUDUpQlJS6hNHT7WZ-6WVkSl_OQC-
oFNCiwVefKGruFNFNmLVQPeabfrWO3wtlJtSl01cOMb2sulXT2YiOP-
3Obxx7WormKwrHayLyZjaiPbc1OwS13TK2tyFtpVyr_nOpKaUn7zytcnrFD0ILreoRd7
5ZA2qSgFwUBgeQkxQfEStdVs2uLP6KIEJ668Db7K98OBzZssGllxaeF1T9yWwgFporj

Regarding cross-border transfer of personal data, such data can be transferred to any country outside Bahrain that the government has whitelisted in the Official Gazette as having an adequate level of data protection.[176] Where a country is not included on this list, a data transfer can be authorized on a case-by-case basis with the regulator taking into account:

> (i) the nature of the data to be transferred, purpose and duration of processing; (ii) the country or territory of origin of the data, its final destination, and available measures, in such countries and territories, to protect personal data; and (iii) [r]elevant international agreements and legislations that are in force in the country or territory, which the data shall be transferred to.[177]

The authorization "may be conditional or for a certain timeframe."[178] All notifications and any authorizations granted by the regulator are maintained in a register.[179]

Bahrain has also adopted various laws and regulations entailing data safeguards for the data-driven economy, including a law on cybercrimes,[180] as well as electronic transactions and electronic transferable records.[181] Notably, Bahrain has adopted a unique enabling

---

uBr4X-5uHn3fTdzHxP0By3kwjw!!/ [https://perma.cc/V@GT-YAKA] (setting the rules and procedures for processing sensitive personal data).

176 *Personal Data Protection Law, Law No. (30) of 2018, art. 12 (2018) (Bahr.), http://www.pdp.gov.bh/en/assets/pdf/regulations.pdf [https://perma.cc/B99F-DJMJ].*

177 *Id.*

178 *Id.*

179 *Id.* art. 16; *see also* Transfer of Personal Data Outside the Kingdom of Bahrain, Resolution No. (42) of 2022 (Bahr.), http://www.pdp.gov.bh/en/assets/pdf/executive-decisions/eng/trans-order-countries-and-territories-with-adequate-protection-en.pdf [https://perma.cc/G4DP-HRZW] (regarding the transfer of personal data outside the Kingdom of Bahrain).

180 *See generally* Information Technology Crimes, Law No. (60) of 2014 (Bahr.), https://www.asianlaws.org/gcld/cyberlawdb/GCC/Law%20on%20Combating%20Cybercrime%20in%20the%20Kingdom%20of%20Bahrain.pdf [https://perma.cc/4MV4-ETK2].

181 See *Electronic Transactions, Law No. (28) of 2002, art. 2 (Bahr.), https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/bh/bh057en.pdf [https://perma.cc/D3AZ-J3WS]; Electronic Transferable Records Law, Law No. (55) of 2018, art. 2 (Bahr.), https://bahrainbusinesslaws.com/laws/electronic-transferable-records-law [https://perma.cc/K59Z-67J2].*

framework for the cloud computing industry.[182] This law provides that customer content in cloud computing services located in Bahrain is exclusively governed by the laws of the customer's domicile, thus bypassing several of the difficulties associated with data access for regulatory supervision and law enforcement.[183] If a foreign court issues an order to a service provider based in Bahrain to access customer data, the Attorney General can act upon it as long as the foreign order is legally valid.[184] The Bahraini government has also focused on an integrated policy for opening up government data, including providing detailed mechanisms for releasing such data in an interoperable, machine-readable format.[185] Similarly, the national cybersecurity strategy addresses various aspects of enabling cyber defenses and protecting critical national infrastructure.[186] Bahrain has also promoted the use of the cloud by all government entities through the Cloud First Policy 2017 and Digital Government Strategy 2022, and the country has set out the objective of developing a successful digital economy through the e-Commerce National Strategy (2019–2022).[187]

Bahrain has been active in various multiple international fora, including signing FTAs with the United States, Singapore, and

---

182 *See generally* Providing Cloud Computing Services to Foreign Parties, Decree No. (56) of 2018, § 2 (Bahr.), https://bahrainbusinesslaws.com/laws/Law-of-Providing-Cloud-Computing-Services-to-Foreign-Parties [https://perma.cc/G6MK-CLE6].

183 *Id.* § 3(1).

184 *Id.* § 3(4).

185 *See* Info. & eGovernment Auth., *Open Government Data Policy*, § B (2023) (Bahr.), https://www.iga.gov.bh/Media/Pdf-Section/National%20Digital%20Policies/Open%20Data%20Policy%20V1.3.pdf [https://perma.cc/G54M-Q8LH] (describing the guidelines and procedures public entities must follow regarding the data they generate and collect).

186 *Bahrain National Cyber Security Strategy*, NAT'L CYBER SEC. CTR., https://www.ncsc.gov.bh/en/national-strategy.html#:~:text=Vision,to [https://perma.cc/QJ9X-GABY] (last visited Mar. 29, 2024).

187 *Bahrain's Digital Government Strategy to Unlock Digital Transformation for Public and Private Sectors*, EXPONENTIAL DIGIT. SOLS. (Sept. 13, 2022), https://10xds.com/news/bahrains-digital-government-strategy/ [https://perma.cc/5BK4-G6Z6]; *eCommerce National Strategy*, MINISTRY OF INDUS. & COM., https://www.moic.gov.bh/en/node/2854 (last visited Apr. 1, 2024); *see also* Info. & eGovernment Auth., *Cloud First Policy: General Directorate of Governance and Operations*, 3 (2017) (Bahr.), https://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf [https://perma.cc/D3S2-KBP8].

EFTA states.[188] It is also a participant in the joint initiative on e-commerce at the WTO.[189]

G. Morocco

Morocco was one of the early starters in implementing a data protection law; however, the government is now working towards modernizing the law to make it consistent with the GDPR.[190] The primary law on data protection is set out in Law No. 09-08 of 2009.[191] The law applies to any processing of personal data when it is carried out by entities in Moroccan territory or where the controller (if located outside Morocco) uses personal data of Moroccan residents (except for operations that only require transit).[192] The following kind of data processing falls outside the scope of the law: processing for domestic activities; processing for public security, defense and national security; processing authorized by law; and collection and processing to prevent crime (but subject to certain notification requirements to the privacy regulator).[193]

The law sets out various high-level applicable obligations for processing personal data, such as lawful and fair processing,

---

[188] *See, e.g.*, United States-Bahrain Fair Trade Agreement, Bahr.-U.S., Sept. 14, 2005, https://crsreports.congress.gov/product/pdf/RS/RS21846 (last visited Apr. 1, 2024); Gulf Cooperation Council (GCC)-Singapore Free Trade Agreement & Economic Integration Agreement, GCC-Sing., Dec. 15, 2008, https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/-/media//ESG/Files/Non-Financial-Assistance/For-Companies/Free-Trade-Agreements/GSFTA/Legal_Text/the_gulf_cooperation_council_gsfta_legal_text [https://perma.cc/9BR5-NGC6]; EFTA-Gulf Cooperation Council (GCC) Free Trade Agreement & Economic Integration Agreement, EFTA-GCC, June 22, 2009, https://www.efta.int/media/documents/legal-texts/free-trade-relations/gulf-cooperation-council-GCC/EFTA-GCC%20Free%20Trade%20Agreement.pdf [https://perma.cc/G5NR-AC54]; *EFTA-Gulf Cooperation Council (GCC)*, WORLD TRADE ORG., https://rtais.wto.org/UI/CRShowRTAIDCard.aspx?rtaid=462 [https://perma.cc/G9Q4-HCQ7] (last visited Mar. 1, 2024).

[189] *Joint Initiative on E-Commerce*, *supra* note 170.

[190] Hind Chenaoui, *Moroccan Data Protection Law: Moving to Align with EU Data Protection?*, IAPP (Sept. 11, 2018), https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/ [https://perma.cc/278F-3XBV].

[191] Protection of Individuals with Regard to the Processing of Personal Data, Law No. 09-08 (Feb. 18, 2009) (Morocco). https://www.medical-hospitality-morocco.com/wp-content/uploads/2021/01/Loi-09-08-Fr.pdf [https://perma.cc/F68T-RRUP].

[192] *Id.* art. 2(2).

[193] *Id.* art. 2(4).

purpose specification and limitation, data minimization, and data accuracy.[194] Further, unqualified consent of data subjects is necessary for processing personal data with limited exceptions, such as: where data processing is necessary for compliance with a legal obligation to which the data subject or controller is subject, performance of a contract to which the data subject is a party, safeguarding vital interests of a data subject, public interest, or fulfilment of the legitimate interest pursued by data controller or recipient (subject to the fundamental rights of the data subject).[195] The law also provides data subjects various rights: the right of access, right to rectification, right to object to the processing of personal data, and right to be protected against automated decision-making that has legal effects on the data subject or in the context of a court decision.[196] Processing sensitive data is subject to the prior authorization of the regulator or the express consent of the data subject, subject to certain limited exceptions.[197] The law also sets out specific requirements for processing personal health data.[198]

Regarding cross-border transfers of personal data, a controller may transfer personal data to outside of Morocco if the receiving state has an adequate level of data protection.[199] The regulator will consider the following factors in making an adequacy finding: the legal framework on data protection in the foreign country, public security measures in that country, specific characteristics of data processing and its duration, and the nature and origin of data and destination of data.[200] For certain limited circumstances, the law allows for derogation from the adequacy requirement where the data subject has provided express consent or if the transfer is necessary for specific reasons: (i) safety of data subject; (ii) public interest; (iii) compliance with legal obligations; (iv) performance of a contract between data controller and subject or pre-contractual measures taken at data subject's interest; (v) conclusion and

194 *Id.* art. 3(1).
195 *Id.* art. 4.
196 *Id.* arts. 7–9, 11.
197 *Id.* arts. 12, 21.
198 *Id.* arts. 22, 24.
199 *Id.* art. 43.
200 *Id.*

performance of a contract in the interest of the data subject between the controller and third party; (vi) in international mutual legal assistance; or (vii) for medical reasons.[201] Personal data can also be transferred outside Morocco if there is a bilateral or multilateral agreement to which the Kingdom is a party.[202]

Additionally, Morocco has recently implemented other data regulatory frameworks, including some related to electronic transactions and electronic signatures[203] and cybersecurity, which contain various data safeguards but also come with certain restrictions.[204] Under the cybersecurity law, all sensitive data must be stored in Moroccan territory.[205] Sensitive data is not defined specifically in this law but defined in Law No. 9-08 as data which "reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the person concerned or which relates to their health including their genetic data. . . ."[206] Further, any outsourcing of sensitive information must be the subject of a contract under Moroccan law, which must include commitments to information protection, auditability, and reversibility, as well as security requirements and service levels.[207] A law on critical infrastructure

---

[201] *Id.* art. 44.

[202] *Id.*

[203] See generally *Nat'l Def. Admin.,* Presentation Note of the Law 43.20 on Trust Services for Electronic Transactions *(2020) (Morocco),* https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/presentation%20note%20of%20the%20law%20n%20deg%2043-20%20english%20version.pdf [https://perma.cc/N2ZX-R5JW] *(discussing the adoption and details of Trust Services for Electronic Transactions, Law No. 43.20 (2020) (Morocco)); Electronic Exchange of Legal Data, Law No. 53-05 (2007) (Morocco), https://tahseen.ae/media/3036/law-on-electronic-exchange-of-legal-data.pdf [https://perma.cc/MHG5-B6SB]*.

[204] Cybersecurity, Law No. 05-20 (2020) (Morocco), https://alp.unescwa.org/sites/default/files/2023-03/Cybersecurity%20law%20no%205%202020%20AR.pdf [https://perma.cc/EJ86-AJ4B].

[205] *Id.* art. 11.

[206] Protection of Individuals with Regard to the Processing of Personal Data, Law No. 09-08, art. 1(3) (2009) (Morocco).

[207] Cybersecurity, Law No. 05-20 art. 12 (2020) (Morocco).

also specifies that all sensitive data related to vital infrastructure must be stored on Moroccan territory.[208]

Morocco is a signatory to the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data[209] and Additional Protocol to the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data with Regard to Supervisory Authorities and Transborder Data Flows,[210] as well as the Budapest Convention on Cybercrime.[211] In a side agreement accompanying its FTA with the United States, Morocco also signed ICT Principles that provide for open cross-border data

---

[208] Decree No. 2-15-712 on Protection of Sensitive Information Systems and Infrastructures of Vital Importance, Official Bulletin No. 6458, art. 9 (2016) (Morocco), http://www.sgg.gov.ma/Portals/0/BO/2016/BO_6458_Fr.PDF?ver=2016-05-05-092424-563 [https://perma.cc/Z9GC-V4Y6]. Sensitive data is defined as any data whose manipulation or destruction can impair the continuity of operation or harm the information systems of the vital infrastructure. *Id.* art. 1.

[209] *Support to Data Protection in Morocco*, COUNCIL OF EUR., https://www.coe.int/en/web/data-protection/support-to-data-protection-in-morocco#:~:text=Morocco%20has%20been%20Party%20to,Consultative%20Committee%20of%20Convention%20108 [https://perma.cc/KF8Y-G7AR] (last visited Mar. 1, 2024) ("Morocco has been Party to the . . . Convention for the protection of individuals with regard to automatic processing of personal data . . . since September 2019 . . . ."); *see also* Council of Eur., Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108, https://rm.coe.int/1680078b37 [https://perma.cc/NT4V-5EMY].

[210] *Welcome to Morocco, 55th State Party to Convention 108!*, COUNCIL OF EUR. (May 28, 2019), https://www.coe.int/en/web/data-protection/-/welcome-to-morocco-55th-state-party-to-convention-108- [https://perma.cc/P9AZ-65VK]; *see also* Council of Eur., Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authority and Transborder Data Flows, Nov. 8, 2011, E.T.S. No. 181, https://rm.coe.int/1680080626 [https://perma.cc/2239-8UVX].

[211] *International Conference in Morocco on Strengthening Co-operation on Cybercrime and e-Evidence in Africa*, COUNCIL OF EUR. (Mar. 6, 2023), https://www.coe.int/en/web/deputy-secretary-general/-/international-conference-in-morocco-on-strengthening-co-operation-on-cybercrime-and-e-evidence-in-africa#:~:text=Morocco%20is%20a%20Party%20to,signature%20on%2012%20May%202022 [https://perma.cc/WZ4T-UH6V] ("Morocco is a Party to the Cybercrime Convention since 2018 . . . ."); *see also* Council of Eur., Convention on Cybercrime, Nov. 23, 2011, E.T.S. No. 185, https://rm.coe.int/1680081561 [https://perma.cc/PN9K-GP8C].

flows and prevent data localisation.[212] It is also a party to the Malabo Convention and the Arab States—Convention on Combating Information Technology Offences.[213]

H. Kuwait

In the last few years, Kuwait has extensively legislated in various areas affecting the digital and data economy, although several aspects of the regulatory framework are still evolving or remain unclear. In February 2024, the Communication and Information Technology Regulatory Authority in Kuwait published a new law on data protection applicable to telecommunications and information technology service providers.[214] However, the official English translation of this Regulation is not yet available as of the time of this writing. This new law on data protection repeals the older regulation of 2021.[215] The scope of application of Kuwaiti data protection law is much narrower than most data protection laws worldwide, which apply to private and public sector entities at large, with some exceptions for public entities.[216]

The Cloud Computing Regulatory Framework of Kuwait sets out the details of data classification, categorizing data into Tier 1 (public data), Tier 2 (private insensitive data), Tier 3 (private

---

[212] OFF. OF THE U.S. TRADE REPRESENTATIVE, *Kingdom of Morocco-United States Trade Principles for Information and Communication Technology Services* (2012), https://ustr.gov/sites/default/files/United%20States%20Morocco%20ICT%20Principles.pdf [https://perma.cc/L3PD-VY82].

[213] *The Kingdom of Morocco Ratifies the Malabo Protocol*, PAN-AFRICAN PARLIAMENT (June 7, 2022), https://pap.au.int/en/news/press-releases/2022-06-07/kingdom-morocco-ratifies-malabo-protocol#:~:text=The%20Kingdom%20of%20Morocco%20has%20become%20the,to%20deposit%20instruments%20of%20ratification%20of%20the [https://perma.cc/5ZRS-2KE2]; *see also* League of Arab States, *supra* note 128, at 28 (listing the Kingdom of Morocco as a signatory).

[214] Commc'n & Info. Tech. Regul. Auth., *Data Privacy Protection Regulation*, Reg. 26 of 2024 (Kuwait). *See also Kuwait: CITRA publishes new Data Privacy Protection Regulation 2024*, DATAGUIDANCE (Mar. 13, 2024), https://www.dataguidance.com/news/kuwait-citra-publishes-new-data-privacy-protection [INSERT PERMA].

[215] Commc'n & Info. Tech. Regul. Auth., *Data Privacy Protection Regulation* (Repealed), (2021) (Kuwait).

[216] *See, e.g.*, Council Regulation (EU) 2016/679, General Data Protection Regulation, arts. 2, 3, 2016 O.J. (L 119) 32–33.

sensitive data), Tier 4 (highly sensitive data).[217] This framework contains a data localization requirement, whereby private and business sectors are prevented from hosting Tier 3 and 4 data outside Kuwait.[218] Further, subscribers of cloud computing services must not transfer, store, or process shared content to any public, hybrid, or community cloud, unless the cloud computing service provider is properly registered and licensed by the government.[219] All licensed cloud service providers must disclose to the government their data centers inside and outside of Kuwait.[220] Additionally, Kuwait has several other supporting regulatory frameworks, including electronic transactions,[221] cybercrimes,[222] and electronic payment of funds.[223] Kuwait has also adopted a cloud-first policy to encourage government use of the cloud.[224] The National Cyber Security Strategy provides a roadmap towards strengthening cybersecurity information and taking all the necessary precautions.[225]

---

[217] Commc'n & Info. Tech. Regul. Auth., Data Classification Policy, § 3.3 (2011) (Kuwait), https://www.citra.gov.kw/sites/en/LegalReferences/Data_Classification.pdf [https://perma.cc/WJM3-LGDB].

[218] Commc'n & Info. Tech. Regul. Auth., *Cloud Computing Regulatory Framework*, chs. 3.2.1.2, 4.2.1.1 (2021) (Kuwait), https://www.citra.gov.kw/sites/en/LegalReferences/Cloud_computing_regulatory_framework.pdf [https://perma.cc/DN96-R9YR]; *see also* Commc'n & Info. Tech. Regul. Auth., *Cloud Service Providers Regulations and Commitments*, 11 (2021) (Kuwait), https://www.citra.gov.kw/sites/en/LegalReferences/Cloud_service_providers_regulations_and_commitments.pdf [https://perma.cc/E4Y5-QZ95].

[219] *Cloud Computing Regulatory Framework*, *supra* note 218, ch. 4.2.1.2.

[220] *Id*. ch. 4.2.1.3.

[221] *See generally* Electronic Transactions, Law No. 20 of 2014 (Kuwait).

[222] *See generally* Council of Eur., *Kuwait Cybercrime Legislation* (2020), https://rm.coe.int/octocom-legal-profile-kuwait/16809e5372#:~:text=Each%20Party%20shall%20adopt%20such,%2C%20deleting%2C%20deteriorating%2C%20altering%20or [https://perma.cc/BM9Z-H2SH].

[223] *See generally* Regulating the Electronic Payment of Funds, Resolution No. 45/471 of 2023 (Central Bank of Kuwait); *see also Central Bank of Kuwait's Overhaul of e-Payment Regulations*, AL TAMIMI & CO. (June 19, 2023), https://www.tamimi.com/news/central-bank-of-kuwaits-overhaul-of-e-payment-regulations/ [https://perma.cc/Q94J-HRQP].

[224] Commc'n & Info. Tech. Regul. Auth., *Cloud First Policy*, § 3.1.1 (2021) (Kuwait), https://www.citra.gov.kw/sites/en/LegalReferences/Cloud_first_policy.pdf [https://perma.cc/TWM6-HRYT].

[225] Commc'n & Info. Tech. Regul. Auth., *National Cyber Security Strategy for the State of Kuwait (2017–2020)*, 14 (2017) (Kuwait),

I. Jordan

Jordan also has an emerging framework for cross-border data flows, although several of the laws and regulations were not accessible to us in English. Jordan's Personal Data Protection Law has been recently ratified and strengthens the privacy rights of Jordanian people in the digital context.[226] The law aims to find the right balance between protecting privacy and encouraging the growth of data-driven innovations.[227]

Article 15 of a draft Jordanian law deals with cross-border transfer of personal data.[228] In summary, the law allows for transfer of personal data in the following circumstances: (i) if the data storage is compliant with relevant cybersecurity measures; (ii) if the data transfer in pursuance of a judicial cooperation treaty that Jordan has signed; (iii) if the data transfer is to cooperate with processing and exchange of data related to public health; (iv) if the data transfer fulfils a national interest approved by the Council of Ministers, and (v) if the data subject consents to the data transfer.[229] However, without access to further translations, we are unable to confirm the scope and applicability of the data protection law to cross-border transfer of data.

Jordan has also adopted other regulatory frameworks in the past several years to provide a basic regulatory foundation for the development of the digital and data economy. For instance, it has

---

https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf [https://perma.cc/85KM-DE9L].

[226] Jordanian Personal Data Protection, Law No. (24) of 2023 (the "PDPL") (Jordan), https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf [https://perma.cc/2S74-PJPE]. This law is enforceable starting March 17, 2024. *Id.*

[227] Ministry of Digit. Econ. & Entrepreneurship, *The National Digital Transformation Strategy & Implementation Plan (2021–2025)*, 19 (2021) (Jordan), https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/dts-2021-eng.pdf [https://perma.cc/48UZ-FSVS].

[228] *Data Protection Laws of the World: Jordan*, DLA PIPER, https://www.dlapiperdataprotection.com/index.html?t=law&c=JO [https://perma.cc/PD3K-MCLB] (last modified Jan. 11, 2024).

[229] *Id.*

implemented a law on cybercrimes,[230] electronic transactions,[231] cybersecurity,[232] and electronic payments.[233] None of these frameworks contain specific requirements or obligations for cross-border data flows, but they provide safeguards necessary to enable data flows.

The recently implemented Cloud (Services & Platforms) Policy 2020, applicable to all government entities benefitting from any kind of cloud services, sets out a data classification policy, where all data can be classified into: (i) Secret (such data has to be stored in the country in secure data centers); (ii) Sensitive (stored in Jordan, although different kinds of data centers can be used, including those of the private sector; these data centers are limited to SaaS providers); (iii) Private (such data can be stored inside or outside the Jordan with different cloud service providers, although data storage by private sector can be restricted inside or outside the country); and (iv) Ordinary (can be stored anywhere, different cloud services available, and no other limitations).[234] Along similar lines, the Data Classification and Management Policy 2019 also clearly lays out that the the storage, circulation, and release of government data must be undertaken in a manner that ensures national security and that individuals' privacy is maintained.[235]

---

[230] *See* Hamza Alakaleek, *Jordan's Cybercrime Law—Balancing Security and Rights*, JORDAN NEWS, https://www.jordannews.jo/Section-36/Opinion/Jordan-s-cybercrime-law-balancing-security-and-rights-29828 [https://perma.cc/3VVJ-ES69] (July 20, 2023).

[231] *See generally* Electronic Transactions Law, Law No. (15) of 2015 (2015) (Jordan), https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/bec70415-2845-42df-bc47-5e0ee4b859b7.pdf (last visited Apr. 1, 2024).

[232] *See* Sevan Araz, *Jordan Adopts Sweeping Cybersecurity Legislation*, MIDDLE E. INST. (Jan. 30, 2020), https://www.mei.edu/publications/jordan-adopts-sweeping-cybersecurity-legislation [https://perma.cc/8S2W-BSJV].

[233] *See generally* Instructions of Financial Consumer Protection for Electronic Payment and Transfer of Fund Companies, No. (3) of 2021 (2021) (Jordan), https://orange.jo/sites/default/files/documents/cbj_ins.pdf [https://perma.cc/2DCZ-NL86].

[234] Ministry of Digit. Econ. & Entrepreneurship, *Cloud (Platforms & Services) Policy 2020*, 6–7 (2020) (Jordan), https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/cloudpolicy-2020-english.pdf [https://perma.cc/HE5P-LLEX].

[235] Ministry of Digit. Econ. & Entrepreneurship, *Data Classification & Management Policy*, § 2 (2019) (Jordan),

The government has also expressed interest in encouraging the use of open government data to enable digital innovation in the country, highlighting principles of openness-by-default, non-discrimination, timeliness, and transparency.[236] In a document accompanying its FTA with the United States, Jordan has committed to high-level principles of open networks and cross-border data flows (like Morocco).[237] It is also party to the League of Arab States—Convention on Combating Information Technology Offences.[238]

J. Djibouti

Our desktop research did not provide information regarding any specific regulatory frameworks on cross-border data flows.[239] Several of the recommendations set out in our conclusion will be relevant for Djibouti in setting their regulatory framework on data governance.

Figure 2 below provides a summary of the cross-border data regulations for Saudi Arabia, Rwanda, Pakistan, Oman, Nigeria, Bahrain, Morocco, Kuwait, and Jordan.

Saudi Arabia[240]	• Broad number of data localization requirements, including personal data. • Sensitive personal data cannot be transferred abroad. • Strict localization requirements for government data and overriding national security considerations. • Strong regulation of emerging technologies, IoT, cloud computing, etc.

https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/EB_List_Page/Data_management_and_classification_policy.pdf [https://perma.cc/MCN5-2TLJ].

236 *Ministry of Info. & Commc'ns Tech.,* Open Government Data Policy, § *2-1 (2017) (Jordan)*, https://portal.jordan.gov.jo/OGD-Policy_en.pdf [https://perma.cc/D2LY-69V5].

237 William M. Daley & Mohammed Halaiqah, US-Jordan Joint Statement on Electronic Commerce, http://www.sice.oas.org/Trade/us-jrd/St.Ecomm.pdf [https://perma.cc/QU3A-WEDR].

238 League of Arab States, *supra* note 128, at 27 (listing the Hashemite Kingdom of Jordan as a signatory).

239 *See Djibouti: Data Protection Factsheet*, *supra* note 6.

240 *See supra* notes 35–60 and accompanying text.

	• Sector-specific data localization requirements in banking, IoT, tax law, etc. • Encouraging a strong culture of cybersecurity and protecting critical infrastructure. • Ambition to foster the benefits of open data and digital economy. • Restricted engagement with international initiatives on cross-border data flows till date.
Rwanda[241]	• Extensive requirements for data localization, often to satisfy digital industrialization-related objectives. • Data localization requirement of personal data. • Focus on data sovereignty as a policy objective. • Active participant in regional initiatives in Africa. • Focused on building and fostering domestic data economy including open government data initiatives.
Pakistan[242]	• Emerging framework on data governance, e.g., developing data protection bill. • In the process of developing domestic data protection law; proposed localization of critical personal data. • Sustained focus on building domestic e-commerce sector and e-payments sector. • Migrating government bodies to the cloud and digitalizing government departments.

241 *See supra* notes 61–84 and accompanying text.
242 *See supra* notes 85–101 and accompanying text.

	• Limited international engagement to date.
Oman[243]	• Focus on online content regulation, especially VoIP services. • Development of domestic data centers and capabilities. • Government data must enable open data initiatives. • Important role of Cyber Defense Centre in data governance. • Sustained engagement with trading partners in the Middle Eastern region on digitalization.
Nigeria[244]	• Sustained focus on driving indigenous data-driven innovation, including through data localization measures. • Adequacy-like framework for transfer of personal data, subject to the supervision of the Attorney General. Limited exceptions apply. • Extensive development of a new data protection law, similar framework for cross-border data transfers as the GDPR. • Interlinkage of national security, cybersecurity and sovereignty in various policy frameworks. • Strong data localization requirements for government data, telecommunications-related data. • Obligation to peer internet traffic using local ISPs. • Active participation in regional initiatives and at the WTO.

243 *See supra* notes 102–130 and accompanying text.
244 *See supra* notes 131–170 and accompanying text.

Bahrain[245]	• Focus on developing an open and secure framework for cross-border data flows that maximize opportunities for e-commerce. • Whitelisting or adequacy-based approach for cross-border data transfer. • Authorization route available for non-whitelisted countries. • Extensive rights granted to data subjects, but no right to data portability. • Comprehensive and updated framework on electronic transactions, electronically transferable records. • Mechanism to enable customer data access based on domicile for locally hosted cloud data. • Multi-pronged cybersecurity strategy focused on cyber defense and national critical infrastructure. • Geared towards government digitalization and open data policies. • Active participant in regional and international fora.
Morocco[246]	• Early starter on data protection law but need to upgrade to GDPR standards. • Predominantly based on adequacy-based framework with some derogations. • Data localization requirement for sensitive data in cybersecurity and critical infrastructure laws/decrees, no such requirement in data protection law.

[245] *See supra* notes 171–189 and accompanying text.
[246] *See supra* notes 190–213 and accompanying text.

	• Only DCO member to Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and its updated version. • Continued engagement with Arab regional groups and African Union.
Kuwait[247]	• Narrow scope of application of data protection law to telecommunication services and related providers. • Elaborate system of data classification; cloud computing guidelines developed around the data classification policy. • Basic frameworks on electronic transactions, cybercrimes, etc. in place. • Limited international engagement outside the Arab region.
Jordan[248]	• Still a nascent framework for cross-border data flows. • Data protection law in the works; some references in other domestic laws and regulations. • Data classification policy in place; localization requirement for secret and sensitive data. • New initiatives on open government data. • Limited international engagement on global or regional cross-border data flow initiatives to date.

Figure 2: Cross-Border Data Flows Regulatory Framework Highlights

247 *See supra* notes 215–225 and accompanying text.
248 *See supra* notes 226–238 and accompanying text.

III. POLICY RECOMMENDATIONS: HOW DCO MEMBERS CAN OPTIMIZE THEIR FRAMEWORKS ON CROSS-BORDER DATA FLOWS

This Part establishes our mapping exercise, focusing on the significant aspects of cross-border data flow regulation in the context of digital trade for DCO members. The mapping exercise indicates that while several DCO countries have adopted comprehensive domestic laws and policies (especially in the past few years), certain gaps remain. Further, while most DCO countries have focused on developing data enabling mechanisms and strengthening data safeguards, data restrictions are also common. As we proposed in Part I, an optimal regulatory design for cross-border data flows must incorporate three elements: facilitate data enablers, improve data safeguards, and minimize data restrictions. In the context of the regulatory experience of the DCO members, we set out some high-level recommendations below for DCO Members to consider based on this framework.

A. Facilitating Data Enablers

Data enabling mechanisms will play a critical role for DCO members to facilitate rapid digital transformation. These mechanisms can play a key role at the domestic and international/regional level.

At the international level, our key recommendations for DCO Members are:

a. DCO Members must actively engage in regional negotiations to create mechanisms for cross-border data flows for the purposes of digital trade. DCO Members are already part of common forum such as the AfCFTA and the Arab League,[249] which can act as important sites for developing best-in-class practices in digital trade, including data certification mechanisms and code of conduct for cross-border data flows. These practices and

---

[249] *See State Parties*, *supra* note 166 (listing state parties in the AfCTA); Country Data, LEAGUE OF ARAB STATES, http://www.leagueofarabstates.net/en/aboutlas/Pages/CountryData.aspx (last visited Apr. 1, 2024) (listing parties in the Arab League).

mechanisms can be implemented at a regional level, with the DCO playing an important unifying role. For example, under the AfCFTA, DCO members could negotiate a protocol for enabling data flows within the African Union.

b. DCO Members can also update their regulatory frameworks (e.g., on data protection)[250] to participate in existing mechanisms such as the CBPR mechanism, which could enable these countries to participate in digital trade activities in the highly dynamic Asia-Pacific region.

c. DCO Members should actively consider participating in digital trade negotiations, both at the WTO (under the Joint Initiative)[251] as well as in e-commerce negotiations at a bilateral or regional level. For instance, Saudi Arabia and Nigeria are already participating in the Joint Initiative on E-commerce at the WTO.[252] Nigeria and Pakistan can highlight important limitations faced by developing countries in developing regulatory frameworks for cross-border data flows for digital trade. Similarly, DCO members may consider negotiating electronic commerce chapters in their FTAs, which would set out broad obligations on enabling cross-border data flows and eliminating data localization measures, subject to reasonable public policy exceptions. So far, most DCO members are behind other countries in negotiating digital trade agreements.

d. DCO Members must actively participate in global and regional initiatives on developing regulatory frameworks, standards, and best practices for data governance. For instance, with most DCO members now implementing (or already having implemented) data protection laws, such members can plan to join the Global Privacy

---

250 *See* discussion *infra* Section III.B.

251 The Joint Initiative on E-commerce at the World Trade Organization is a collaborative effort among WTO members to create rules and regulations that facilitate electronic commerce (e-commerce), with its main focus directed at addressing issues related to digital trade. *See Joint Initiative on E-Commerce*, *supra* note 170.

252 *Id.*

> Assembly (perhaps as observers in the first stage).[253] This may also provide them with the relevant regulatory experience to build stronger domestic privacy and data protection regulatory bodies. DCO members can also update regional conventions on privacy and data convention (including Malabo Convention) to set up a robust regional mechanism to enable cross-border data flows on digital trade. Similarly, DCO members must consider developing cooperative mechanisms to play a more active role in global internet governance, especially by participating and contributing to the relevant technical and policy bodies. Our analysis indicates that there is room for improvement on this front.

At the domestic level, data enablers are critical in maximizing the benefits of cross-border data flows for digital trade. We recommend the following actions from DCO members:

a. Open government data initiatives will play a crucial role in the development of data economies for DCO members. We have already observed in Part II that several DCO members are actively promoting open data portals and adopting principles of openness, non-discrimination, and transparency to facilitate the development of big

---

[253] *See* GLOB. PRIV. ASSEMBLY, https://globalprivacyassembly.org/ [https://perma.cc/K5LQ-LVU4] (last visited Mar. 30, 2024). The Global Privacy Assembly ("GPA") is an international forum for data protection and privacy authorities. *Id.* It provides a platform for its members to collaborate, share information, and set standards for privacy and data protection issues globally. *See Mission and Vision*, GLOB. PRIV. ASSEMBLY, https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/ [https://perma.cc/QJ87-AVUX] (last visited Apr. 1, 2024). The GPA facilitates the exchange of best practices and discussions on emerging privacy challenges and solutions. *Id.* For DCO (Digital Cooperation Organization) members, initially participating as observers in the GPA could be an appropriate step. Being an observer would allow these countries to gain insights into global privacy trends, standards, and regulatory practices without the commitment required of full members. This role can be particularly beneficial for countries still developing or updating their data protection laws. By observing and learning from the experiences and practices shared at the GPA, DCO members can enhance their understanding and capacity to build more robust domestic privacy and data protection frameworks. It's a strategic way to align with international standards while tailoring their approach to fit national needs and contexts.

public datasets. We consider this to be a step in the right direction. Knowledge sharing among DCO members on open data initiatives and implementation of these programs can play an important role in the future. It is also important to tie these open data initiatives with long-term programs on digital inclusion.[254]

b. An important complement to open data governance is clear and precise data classification policies. We observe in Part II that several DCO members have adopted data classification policies in recent years that clearly distinguish between secret and confidential data belonging to the government and other non-sensitive data that can be shared on a global, transparent basis. DCO members that do not currently have such policies must consider the same initiatives because data sharing by governments can be a major driver of data-driven growth for DCO members.

c. Provisions on data interoperability and portability will play a key role in fostering a dynamic environment for data-driven innovation. As we observe in Part II, certain DCO countries have started working on data interoperability standards (still at a nascent stage). Others are still far behind. Similarly, while some countries have included a right to data portability in their domestic data protection laws, others have not yet included this right for their data subjects. Both of these factors will play a

---

[254] This refers to sustained and comprehensive strategies designed to ensure that all segments of the population have access to, and can effectively use, digital technologies and the internet. *See, e.g.*, GLOBAL DIG. INCLUSION PARTNERSHIP, https://globaldigitalinclusion.org [https://perma.cc/Q8KN-FJCM]. These programs typically focus on addressing barriers such as lack of infrastructure, affordability, digital literacy, and accessibility, especially in underserved or marginalized communities. *See, e.g.*, *Policy and Regulatory Good Practices*, GLOBAL DIG. INCLUSION PARTNERSHIP, https://globaldigitalinclusion.org/our-work/policy-and-regulatory-good-practices [https://perma.cc/G64S-TGS5] (last visited Apr. 1, 2024). The goal is to bridge the digital divide, allowing everyone to participate in the digital economy and benefit from digital advancements, including access to information, services, and opportunities for economic and social development. Integrating these programs with open data initiatives can enhance the impact and reach of digital inclusion efforts.

crucial role for more competition in the digital economy. Here, the DCO members must carefully observe the experience of the European Union in developing and implementing frameworks on data interoperability and portability. Co-regulatory initiatives with key private technology players operating in DCO countries could also play a key role.

d. One of our observations in Part II is that several of the regulators in the digital economy are often tied to a specific government Ministry. However, as per the best regulatory practices, independent supervisory authorities (implying both organizational and functional independence) can play a crucial role in fair and objective enforcement of domestic digital laws and regulations. To the extent permissible within their political and legal systems, DCO members must facilitate establishment of independent supervisory authorities, especially for privacy and cybersecurity.

B. Improving Data Safeguards

Data safeguards are fundamental in enabling cross-border data flows. As our examination in Part II indicates, DCO members are heavily engaged in developing appropriate regulatory frameworks related to data governance. It is important that such measures are balanced, proportionate, and implemented transparently and in good faith. Below we set out some key recommendations to improve data safeguards for DCO members:

a. Privacy trustmarks[255] and data certification mechanisms can play a critical role in enabling digital trade and cross-border data flows. DCO members must develop data

[255] A privacy trustmark is a type of certification or seal awarded to organizations, websites, or services that meet certain standards of privacy and data protection. *See* Margaret Rouse, *E-commerce Trustmark*, TECHOPEDIA, https://www.techopedia.com/definition/1491/e-commerce-trustmark (last visited Apr. 1, 2024) (Aug. 19, 2011). It is essentially a visual symbol or badge that indicates compliance with specific privacy practices, reassuring users, and customers that their personal data is being handled responsibly and securely. *Id.*

certification mechanisms (ideally at a regional level) to enable different frameworks for privacy and data protection to interoperate. In this regard, DCO members have an excellent opportunity to explore the development of mutual recognition mechanisms for data protection, given their closely aligned economic and political interests.

b. At the very core of digital regulation lies digital trust. Digital trust can be enabled in domestic laws and regulations by providing digital users with robust rights, protecting them from illegal surveillance and intrusion, and enabling them to participate freely in the digital economy. Therefore, it is important that DCO members adopt domestic laws for online consumer protection, electronic transactions, and cybercrimes consistent with international standards and best practices. For instance, the United Nations Commission on International Trade Law ("UNCITRAL") has developed various frameworks on electronic commerce and electronic transactions, which inform the domestic laws of several countries across the world.[256] Similarly, the Organization for Economic Co-operation and Development ("OECD") has developed best practices for online consumer protection.[257] These best practices could be relevant benchmarks for DCO countries when they are updating or revising their domestic regulatory frameworks. Compliance measures must be reasonable, proportionate, and objective in these domestic digital laws and regulations. Some DCO members have also already signed the Budapest Convention

---

[256] *See, e.g.*, Rep. of the Comm. on Int'l Trade L., at 6, U.N. Doc. A/51/628 (1996); Rep. of the Comm. on Int'l Trade L., at 8, U.N. Doc. A/56/588 (2001); Rep. of the Comm. on Int'l Trade L., at 2, U.N. Doc A/72/114 (2017).

[257] *See generally* Org. for Econ. Co-operation [OECD], *Consumer Protection in E-Commerce: OECD Recommendation* (2016), https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf [https://perma.cc/WYH8-E6ZH].

on Cybercrime and the League of Arab States – Convention on Combating Information Technology Offences.[258]

c. In Part II, we have observed that several DCO members have developed cybersecurity frameworks and strategies for protecting the critical infrastructure within their country and strengthening domestic cyber defense capabilities. To boost the cybersecurity of domestic frameworks and protect the data from cyber intrusion, it remains important that governments work alongside the private sector, especially given their predominant role in devising and implementing cybersecurity standards and solutions.[259] Further, domestic laws and regulations must incorporate relevant international standards (e.g., ISO standards) by reference instead of developing domestic standards, which may not be consistent with international standards. These standards must be implemented in a transparent and objective manner.

d. National security considerations play an important role in cyberspace. In our discussions in Part II, especially in relation to data protection laws, we find that several derogations are possible (for instance, compliance with data protection laws by public entities) for national security considerations. It is important that such derogations are balanced and implemented in a proportionate and reasoned manner to boost digital trust among digital users of the country. Similarly, data protection safeguards must adequately apply to public sector bodies, consistent with the domestic legal framework in each country.

---

[258] *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/parties-observers [https://perma.cc/WN63-8W32] (last visited Mar. 1, 2024); League of Arab States, *supra* note 128, at 27–29.

[259] *See* Raquel Vázquez Llorente, *A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity*, MEDIUM (May 21, 2018), https://lseideas.medium.com/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622 [https://perma.cc/FKH6-X8P7].

e. Adequacy regimes are very common to most data protection laws across the world, including for DCO members.[260] It is important, however, in implementing the adequacy or whitelisting approach for regulators to: (i) provide clear and transparent criteria for making an adequacy finding; (ii) ensure that the process of adequacy determination follows due process and representative in nature; and (iii) provide facilitative mechanisms to ensure that adequacy negotiations are conducted in an efficient manner. Using benchmarks and guidance notes developed by transnational bodies such as the Network of African Data Protection Authorities could be helpful in enabling faster negotiations.

C. Minimizing Data Restrictions

The examination of regulatory frameworks in Part II indicates that most countries adopt data localization as a common tool to protect privacy rights of individuals, to protect national security, and to achieve data sovereignty objectives. Further, some laws contain extensive licensing requirements for digital platforms and telecommunications services operators.[261] We recommend the following measures for DCO members to consider in minimizing the use of data restrictions:

a. Data localization measures, where implemented, must be as narrow and specific as possible. Several studies have indicated that data localization measures create an economic burden for companies, as well as consumers, and do not generate proportional benefits for the domestic economy.[262] Thus, data localization should be chosen as

---

[260] *See, e.g.*, discussion *supra* Sections II.E, II.G (discussing Nigeria and Morocco, respectively).

[261] *See* discussion *supra* Sections II.A, II.B, II.H.

[262] *See, e.g.*, Inst. of Int'l Fin., *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy*, 1 (2020), https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf [https://perma.cc/FM25-JCCJ]; Matthias Bauer et. al., Eur. Ctr. for Int'l Pol. Econ, *The Costs of Data Localization: Friendly Fire on Economic Recovery*, 2 (2014), https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf

a policy tool only where it is absolutely necessary to achieve a policy objective. If other mechanisms are available to achieve the same policy objective and are less restrictive in nature, the alternatives must be considered. Certain DCO members have limited regulatory capacity to implement sophisticated regulatory measures on data flows[263] and may thus prefer data localization instead. In the long run, it is important for the DCO membership to create more coordination and cooperation mechanisms to minimize the adoption of such data restrictive measures.

b. While the digital sector must increasingly be regulated for various reasons, including for cybersecurity-related reasons, it is important that governments consider a careful analysis of various compliance requirements such as licensing and technical standards. To the extent possible, these processes should be transparent, objective, and based on international standards and best practices.

CONCLUSION

The prospects of digital integration for organizations such as the DCO present a unique opportunity for its members to align and find common solutions to several cross-cutting problems on data governance. With specific reference to cross-border data flows, the DCO has immense, untapped opportunity to develop stronger consensus among its members to develop the appropriate cross-border framework on data flows for the purposes of enabling digital trade among members. Various proposals have been set in the previous sections to develop more alignment on boosting data safeguards and data

[https://perma.cc/ZE6K-AN22]; Nigel Cory et al., *The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam*, INFO. TECH. & INNOVATION FOUND. (Dec. 12, 2022), https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/ [https://perma.cc/ED9M-XQ34].

263 *See* discussion *supra* Part II.

enablers while minimizing digital and data restrictions. The DCO can be a harbinger of digital trust.

International cooperation must play a key role in the DCO to foster the benefits of data-driven technologies in an optimal and effective manner. In that regard, several prospects exist for regulatory coordination and developing various mechanisms for data and digital interoperability to enable digital trade opportunities. Further, the DCO can dedicate resources to finding commonalities in the region and facilitate knowledge sharing on several of the issues discussed in this Article, such as open data sharing projects, cross-border enforcement of data-related laws and regulations, implementing data classification mechanisms, and developing certification mechanisms for cross-border data transfers. The DCO can also play a positive role in creating consensus and integrate perspectives on cross-border data flows such that DCO members can take a consolidated position before relevant international bodies such as the WTO, regional trade bodies, and internet governance bodies.