

# **Policy Brief**

## **Developing Interoperability Mechanisms to Enable Cross-Border Data Flows**

December 2023



# TABLE OF CONTENTS

Executive Summary	03
DCO Member States are Prioritizing Development of their Digital Economies	06
Access to Data is Needed for DCO Member States to Grow their Digital Economies and Engage in International Trade	08
Access to Data is also Important for Small Businesses	09
Limits to Cross-Border Data Flows are Costly	09
DCO Member State Data Governance Regulation	12
The Key Drivers of Data Flow Restrictions	14
Interoperability and Cross-Border Data Flows	15
A Data Classification Scheme Amongst DCO Member States	16
Developing Interoperability Mechanisms for Personal Data	17
Different Approaches to Interoperability for Cross-Border Flow of Personal Data	19
Supporting Cross Border Payments	21
Developing Cross-Border Digital IDs	23
Glossary and Abbreviations	24
Contributors	26
Bibliography	27

# EXECUTIVE SUMMARY

Access to and use of data is a key element of the digital economy and it enables international trade. This has made data governance central to any successful policy to support economic growth. Data governance requires regulation that enables access to data and creates trust amongst governments, businesses and consumers who are online in increasingly interconnected ways. Trust will also be required to support cross-border data flows, particularly as international trade and investment rely on data flows as part of e-commerce, participation in supply chains and as businesses use data to add value to their operations.

There is already high-level recognition amongst many governments, including the DCO Member States of the importance of cross-border data flows. During Japan's hosting of the G20 in 2019, Leaders recognized that "data free flow with trust will harness the opportunities of the digital economy." The following year in Saudi Arabia, G20 Leaders noted "the importance of data free flow with trust and cross-border data flows," a formulation also repeated by Leaders during the Italian G20 in 2021 and Indonesian G20 in 2022.

This policy brief follows-on from a DCO report "Enabling Cross-Border Data Flows Amongst the Digital Cooperation Organization Member States" that provides a detailed analysis of DCO Member States, data governance regulations. As shown in that report, there has been significant growth in data governance regulations affecting cross-border data flows. These regulations have been enacted for a range of reasons that include the protection of personal data, content regulation, financial regulation and for national security purposes.

The growth in the DCO Member States data governance regulation raises a key challenge — how to maximize the opportunities from cross-border data flows that are required to grow their digital economies and support international trade, while also achieving legitimate public policy objectives. This policy brief focuses on the opportunities that interoperability mechanisms provide for enabling cross-border data flows while also respecting the DCO Member States' regulatory autonomy. Interoperability mechanisms are an opportunity to preserve the regulatory autonomy to achieve legitimate public policy goals while also enabling cross-border data flows.

In fact, Leader's statements at the G20 and the G7, as well as various bilateral and regional digital economy agreements recognize the opportunity of interoperability mechanisms. For instance, the 2019 Osaka G20 Leaders Declaration says that "we will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development."<sup>1</sup>

Interoperability mechanisms can be granted unilaterally when one government recognizes another country's regulation as equivalent, in that the regulation achieves the same or similar goal, thereby allowing cross-border data flows. More often, interoperability is by mutual agreement in which arrangements are put in place to support cross-border data flows while also respecting the regulatory differences between countries. Examples of interoperability mechanisms are the US-EU Privacy Shield 2.0, APEC Cross-Border Privacy Rules and ASEAN Model Contractual Clauses.

**This policy brief focuses on the steps that the DCO Member States and the DCO General Secretariat can take to develop interoperability mechanisms. The main policy recommendations are the following:**

- a. Build trust and a community of practice amongst the DCO Member States by developing cooperative projects such as around privacy enhancing technologies that can enable data flows and protect privacy.
- b. The DCO Secretariat should develop an online repository of all DCO Member State regulations affecting cross-border data flows.
- c. Agree on common data governance principles, which can act as a baseline for domestic regulation and build trust in how data will be treated in other DCO Member States, further supporting cross-border data flows.
- d. Develop a common data classification scheme amongst DCO Member States. Agreement on data classification can support interoperability mechanisms and guide businesses holding data on how to classify data and understand its risks.
- e. Develop interoperability mechanisms with an initial focus on enabling flows of personal data by doing the following:
  - i. The DCO Member States should articulate what is required for an adequacy finding under their privacy laws that would allow cross-border data flows.
  - ii. The DCO Member States should assess the likelihood of successfully getting a GDPR adequacy finding from the European Commission to enable flows of personal data between its European member(s) (currently Cyprus) and other DCO Member States, as well as assess the validity of binding corporate rules and standard contractual clauses as alternative mechanisms enabling flows of personal data under GDPR.
  - iii. The DCO Member States should in parallel develop an everyone but EU members strategy for enabling flows of personal data amongst DCO Member States that is more flexible than GDPR.
- f. DCO Member States should develop other flexible interoperability privacy mechanisms. This could include:
  - i. The government-led scheme that business can opt-into when they can demonstrate protection of personal data consistent with other DCO Member State privacy policies.
  - ii. The certification scheme for businesses that demonstrate privacy policies consistent with commonly agreed privacy principles.
  - iii. The agreement on standard contractual clauses that when included in contracts with third parties are deemed consistent with agreed privacy principles or other DCO Member State privacy policies.

Enabling data flows to support cross-border payments is also a priority for many DCO Member States, particularly given the role of payments in supporting digital economy and trade outcome. Enabling cross-border payments at the retail and wholesale levels can reduce costs of international e-commerce and expand opportunities for businesses to participate in cross-border digital trade. **There are a range of steps that the DCO Member States could take to facilitate cross-border payments. Key recommendations are:**

- a. Modernize the regulation on consumer protection, privacy and financial sectors to achieve trust and security that is predictable and appropriate to the risks posed by the provision of electronic payment services.
- b. Encourage innovation and competition in electronic payment services.
- c. Make publicly available regulations on electronic payments, including in relation to regulatory approvals, licensing requirements, procedures and technical standards.
- d. Avoid arbitrarily or unjustifiably discriminating between financial institutions and non-financial institutions in relation to access to services and infrastructure necessary for the operation of electronic payment systems.
- e. Adopt, for relevant electronic payment systems, international standards for electronic payment messaging, such as the ISO 20022 Universal Financial Industry Message Scheme, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems.
- f. Facilitate the use of open platforms and architectures such as tools and protocols provided for through Application Programming Interfaces (APIs) and encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments.

The DCO Member States are also developing digital IDs and the recognition of digital IDs across borders that would support growth in their digital economies and international trade.

**Steps that the DCO Member States could take to enable cross-border recognition of digital IDs are the following:**





- a. Establish frameworks to foster technical interoperability or common standards between each DCO Member State on IDs.
- b. Provide comparable protection of digital IDs afforded by each DCO Member State's respective legal frameworks, or the recognition of their legal and regulatory effects, whether accorded autonomously or by mutual agreement.
- c. Exchange knowledge and expertise on best practices relating to digital ID policies and regulations, technical implementation and security standards, and user adoption.



## DCO Member States are Prioritizing Development of Their Digital Economies

Many DCO Member States are adopting digital transformation programs to achieve economic diversification, create more jobs for their young populations, and maximize the opportunities of data and digital technologies across their economies. Realizing this vision will require developing a regulatory environment that builds trust and enables access to data and cross-border data flows. To this end, the DCO Member States have developed digital economy policies. The following table outlines key policies across **10 DCO Member States**.

DCO Member State	Digital Economy Policy
<b>BAHRAIN</b> 	<p>Aims to be a leading digital economy focusing on cloud computing and ICT infrastructure<sup>2</sup>. The global ICT market in Bahrain was valued at US\$3.81 billion in 2022 and is expected to grow at a compounded annual growth rate (CAGR) of %10.57 to reach a value of US\$6.30 billion by 2027. The cumulative revenue generation opportunities for ICT market in Bahrain are estimated at US\$ 29.41 billion between 2022 to 2027<sup>3</sup>.</p>
<b>CYPRUS</b> 	<p>Digital Strategy for Cyprus 2020-2025 foresees Cyprus to become a fit-for-the-future society and knowledge-based economy enabled by digital and emerging technologies that will drive sustainable economic growth, social prosperity and international competitiveness<sup>4</sup>. Cyprus's Recovery and Resilience Plan (RRP) 2021, to be completed by 2026, includes significant investments of around €282 million, devoting 23 percent of the total cost to digital objectives.<sup>5</sup></p>
<b>JORDAN</b> 	<p>Jordan's Modernisation Vision 2022<sup>6</sup> aims to increase national GDP contribution of the Digital Economy and ICT sector from JD0.9 billion (US\$1.27 billion) in 2021 to JD3.9 billion (US\$5.5 billion) by 2033. Similarly, the ICT exports that stood at JD200 million (US\$280 million) in 2021 are targeted to grow up to JD4.5 billion (US\$6.34 billion) by 2033. Jordan's Council of Ministers has established a National Digital Transformation Committee that partners with the private sector to support entrepreneurship and expand access to digital services.<sup>7</sup></p>
<b>KUWAIT</b> 	<p>Is aiming to increase broadband speeds and is focusing on Smart Cities, while also creating an integrated ecosystem for technology, innovation and knowledge that includes better use of data<sup>8</sup>.</p>
<b>MOROCCO</b> 	<p>Morocco's digital transformation strategy "Digital Morocco"<sup>9</sup> 2025 frames digitalization as a strategic lever for development.<sup>10</sup></p> <p>The Agence de Développement du Digital (Agency for Digital Development) – ADD is responsible for implementing the strategy and devising digital development initiatives. The agency's roadmap is structured around 15 projects to support the digital transformation of Morocco through improving quality of public services, strengthening digital ecosystem and innovation, and reducing the digital divide.<sup>11</sup></p>
<b>NIGERIA</b> 	<p>Nigeria's Digital Economy Development Department is supporting the growth in Nigeria's digital economy, including improving exchanges of digital goods and services and increasing the use of digital technologies across the economy.<sup>12</sup></p>

DCO Member State	Digital Economy Policy
OMAN 	Is focused on digital transformation and using data to improve the efficiency and productivity of the public and private sectors. <sup>13</sup> Digital transformation initiatives related to Oman Vision 2040 <sup>14</sup> should boost the ICT market to OMR 2.2 billion (US\$5.6 billion) in 2024. <sup>15</sup>
PAKISTAN 	Is focused on digitization and building a knowledge economy to build on its already world class IT talent <sup>16</sup> . Pakistan's digital transformation could add PKR9.7 trillion (US\$59.7 billion) of economic value annually in Pakistan's economy by 2030. <sup>17</sup>
RWANDA 	Rwanda's Vision 2050 emphasizes on building a knowledge intensive economy that is driven by data and excels in R&D and innovation. <sup>18</sup> The government aims to triple the representation of its GDP in the technology industry, from current 3 percent to 10 percent over the next decade <sup>19</sup> . The National Strategy for Transformation (NST1) 2017-2024 <sup>20</sup> includes enhancing digital literacy and increasing the uptake of digital financial services as key strategic interventions to boost digital economy.
SAUDI ARABIA 	Saudi Arabia Vision 2030 is focused on digital transformation that includes digital infrastructure, improving the quality and use of data and expanding the use of emerging technologies. <sup>21</sup> ICT spending in Saudi Arabia is forecast to grow at annual compound rate of 9.2 percent between 2019- 2024 and reach US\$46.6 billion <sup>22</sup> .

**For many DCO Member States, an important element of developing their digital economy is the use of digital IDs.** Digital IDs support e-commerce by allowing customers to be identified and to transact across borders. This includes Bahrain, Kuwait, Oman and Saudi Arabia<sup>23</sup> in the Gulf, as well as Morocco,<sup>24</sup> Cyprus,<sup>25</sup> Nigeria, Rwanda,<sup>26</sup> Jordan,<sup>27</sup> and Pakistan.<sup>28</sup> For example, Nigeria has reached nearly 90 million enrollees in its World Bank-funded Nigeria Digital Identification for Development (ID4D) project, with a goal of enrolling 140 million people by 2024, 65 million of whom should be women and girls.<sup>29 30</sup> Some Member States are also linking their digital ID systems. For instance, Bahrain's Information & e-Government Authority (iGA) and the Saudi Data and Artificial Intelligence Authority (SDAIA) are aiming to integrate their ID verification systems, which would streamline commercial and investment procedures between the two countries.<sup>31</sup>

**Interlinking digital payment systems is another goal for many DCO Member States.** Currently, cross-border payments are often expensive with delays, relying on chains of banks for cross-border transactions to be completed.<sup>32</sup> Linking cross-border financial payments will enable e-commerce and have an important development angle. For instance, where increasing access to digital payment services can substitute for credit cards that require bank accounts as well as reduce the costs of remittances. Various DCO Member States are bilaterally linking payment systems, such as project Aber between the Saudi Central Bank- SAMA and the Central Bank of the UAE, as well as regional payments linking arrangements such as the Gulf Payments Company and AFAQ platform that support transfers between SAMA and the Central Bank and other financial institutions of Bahrain and Kuwait. However, only about ten percent globally of payment systems participate in interlinking arrangements, highlighting the scope for progress.

## Access to Data is Needed for DCO Member States to Grow their Digital Economies and Engage in International Trade

Data is foundational for digital economies and for engaging in digital trade. The OECD notes that the creation of economic and social value increasingly depends on the ability to move and aggregate data across a number of locations scattered around the globe.<sup>33</sup> According to the McKinsey Global Institute, global data flows grew at nearly 50 percent per annum between 2010-2019, and around 40 percent annually between 2019-2021.<sup>34</sup> The ability to exchange data across borders is also a key enabler of international trade in four ways:

01

To engage in cross-border e-commerce, business must collect customer data, and fast and cost-effective digital payments are needed to complete cross-border e-commerce transactions. Efficient customs and delivery services rely on cross-border data flows to track and trace goods to their destination.

02

Global supply chains require cross-border data flows. The World Bank has highlighted the role of data flows along supply chains to manage production schedules, respond to changes in consumer demands and to track and trace products across global production networks.

03

Services are increasingly being delivered online, which requires data to flow across borders. Global trade in digitally deliverable services tripled from US\$1.2tn in 2005 to US\$3.2 trillion in 2019, comprising 52 percent of global services trade.<sup>35</sup> Data is also being increasingly used to support research and development globally. For example, sharing data sets and results, including the use of cloud-based artificial intelligence amongst researchers globally enabled rapid development of vaccines for COVID-19.<sup>36</sup> Access to large data sets remain a key input to developing AI systems, further highlighting the importance of cross-border data flows.<sup>37</sup>

04

Data collection and analysis is also being used by business to add value to traditional goods exports.<sup>38</sup> Data is also an increasingly key input into manufacturing operations. Data-driven manufacturing opportunities include using data and machine learning to train robots, using data to deepen insights into operations and increasing efficiencies from the factory floor to warehousing and distribution.



## Access to Data is also Important for Small Businesses



Many of the opportunities of cross-border data flows are particularly pronounced for small businesses<sup>39</sup> and the costs of restricting access to data are potentially most impactful on small businesses. For instance, data flows allow access to a global market for small businesses.<sup>40</sup> This includes access to global business services inputs which increasingly reside in the cloud, including business softwares and professional services platforms

that provide small businesses with access to talent globally.

According to the World Bank, “platform-based business models are increasingly important in low and middle-income countries.”<sup>41</sup> This includes allowing businesses in developing countries to benefit from the services offered on the global market and to provide data intensive services in return.<sup>42</sup>

## Limits to Cross-Border Data Flows are Costly

Data regulation limits and in some cases prohibits cross-border data flows. The following analyzes some of the costs of these regulatory constraints. To start with, restrictions on data flows affect macroeconomic outcomes and like tariffs, raises costs and creates deadweight economic loss. The US International Trade Commission in 2014 estimated that the GDP of the United States would be 0.1percent to 0.3percent higher if data flow restrictions were removed. Similarly, for the European Union, barriers



to transborder data flows are estimated to reduce GDP by 0.4 percent to 1.1 percent, depending on the strength of data localization requirements.<sup>43</sup>



The negative impact of restrictions on cross-border data flows have also been modeled. According to one economic model adopted by the Information Technology and Innovation Foundation (ITIF), a one-unit increase in a country's Data Restrictiveness Index (calculated using data from the OECD Product Market Regulation database) was associated with a 7 percent decrease in gross output traded, a 2.9 percent decrease in the productivity of downstream industries, and a 1.5 percent increase in the price of goods and services from these industries, such as finance and insurance, petroleum, computers and electrical equipment, and chemicals.<sup>44</sup> The authors bolstered these conclusions with case studies in China, Indonesia, Russia and South Africa, which showed that increases in data restrictiveness over a period of five years (2013 to 2018) led to losses in trade and productivity.<sup>45</sup>

Another study assessed the potential GDP impact on 25 countries of removing restrictions on cross-border data flows. The study found that on average, service imports would increase by five percent, benefitting domestic companies and consumers through access to cheaper and better international services.<sup>46</sup> A follow-up study, which measured potential gains for productivity concluded that lifting restrictions on data flows could lead to an average increase in Total Factor Productivity of 4.5 percent.<sup>47</sup>

Limits on cross-border data flows can also have firm level costs by increasing access to key digital technologies that can negatively impact the ability to innovate and be competitive. One report found that "efficiency losses from data localization measures can increase the costs of data hosting by 30 to 60 percent."<sup>48</sup> Limits on access to data raise costs for firms and hinder firm's capacity for global collaboration and innovation.

Insights into the costs of restricting data flows can be obtained from the operation of the EU GDPR, which restricts flows of personal data between the EU and third countries. The economic impacts of the GDPR have been significant. A July 2018 survey of 539 Mergers and Acquisitions professionals from Europe, Africa, and the Middle East revealed that 55 percent had worked on transactions that did not go through due to concerns about companies' compliance with the GDPR.<sup>49</sup>

Looking at the impact of the GDPR within the EU, a study of 1,084 diverse online firms found that since the GDPR was adopted, companies catering to European consumers experienced a 12 percent reduction in website pageviews (implying 15,043 fewer pageviews per week for the median site), as e-commerce sites saw their online revenue drop by 13.3 percent (or US\$9,227 per week for the median site). Indeed, during the first year of GDPR implementation it was found that profit grew 1.7–3.4 percentage points less than those of

their US counterparts, underscoring the impact of restrictions on data flows on small business.<sup>50</sup> While data flow restrictions have costs associated with them, it is also not the case that no data restrictions are optimal. Data governance regulation is needed to ensure privacy, consumer protection, and national security etc. The G20 notion of data free flow with trust directly speaks to the need for regulation. Indeed, data flow restrictions should be understood as a consequence of achieving a particular policy goal than an end.

From this perspective, the question facing the DCO Member States is how best to achieve legitimate domestic goals while limiting the impact on cross-border data flows and access to data. Different countries will balance these goals differently, and therefore there is no one-size fits all approach. As a result, data governance regulation will vary amongst DCO Member States, underscoring the need for interoperability mechanisms.





## DCO Member State Data Governance Regulation

Amongst the DCO Member States, there has been significant cumulative growth in the regulation of cross-border data flows. As can be seen in Figure 01, data flow regulations amongst DCO Member States have grown from one in 2007 to 45 in 2022. Moreover, growth in data flow regulations has accelerated from 28 in 2020 to 45 in 2022, a 60 percent increase over two years.

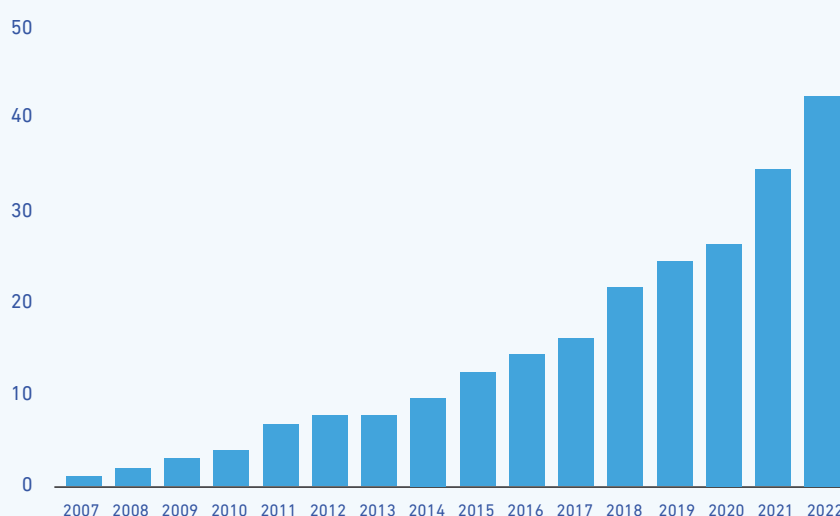


Figure 01: Cumulative Growth in Number of Cross-Border Data Flow Regulations

The following assesses the restrictiveness of DCO Member State data regulation using the World Bank taxonomy of data flow models. As outlined below, these are the **Limited** Transfers Model, the **Conditional** Transfers Model and the **Open** Transfers Model.

**TABLE 01: Laws and Regulations of the DCO Member States Which Affect Cross-Border Data Flows**

REGULATORY OPTIONS	Limited Transfer Models			Conditional Transfer Model	Open Transfer Model
	Local Storage	Domestic Processing	Government Approval	Regulatory Safeguards	Regulatory Safeguards
KEY FEATURES	Broad requirements to use domestic servers for data storage	Broad requirements to use domestic servers for data processing	Prior approval is required for data transfers	<ul style="list-style-type: none"> <li>• Consent</li> <li>• Adequacy findings</li> <li>• Private sector assessment</li> </ul>	<ul style="list-style-type: none"> <li>• No a priori mandatory requirements</li> <li>• Private sector accountability based on voluntary standards</li> </ul>
EXAMPLES	<ul style="list-style-type: none"> <li>• Central Bank of Nigeria Data Requirements</li> <li>• Oman Cloud Governance Framework</li> </ul>	<ul style="list-style-type: none"> <li>• Guidelines for Nigerian Content Development in ICT</li> <li>• Pakistan Prevention of Electronic Crimes Act, 2016 ("PECA 2016")</li> </ul>	<ul style="list-style-type: none"> <li>• Saudi Arabia Cloud Computing Regulatory Framework (CCRF)</li> </ul>	<ul style="list-style-type: none"> <li>• Bahrain Personal Data Protection Law No. 30</li> <li>• European Union General Data Protection Regulation</li> <li>• Saudi Arabia's Personal Data Protection Law ("PDPL") of 2021 amended March 2023</li> <li>• Jordan's Personal Data Protection Law No. 24 of 2023</li> </ul>	<ul style="list-style-type: none"> <li>• Oman Personal Data Protection Law</li> </ul>

More data closure

Less data closure

Source: Based on a diagram from World Bank Development Report 2021



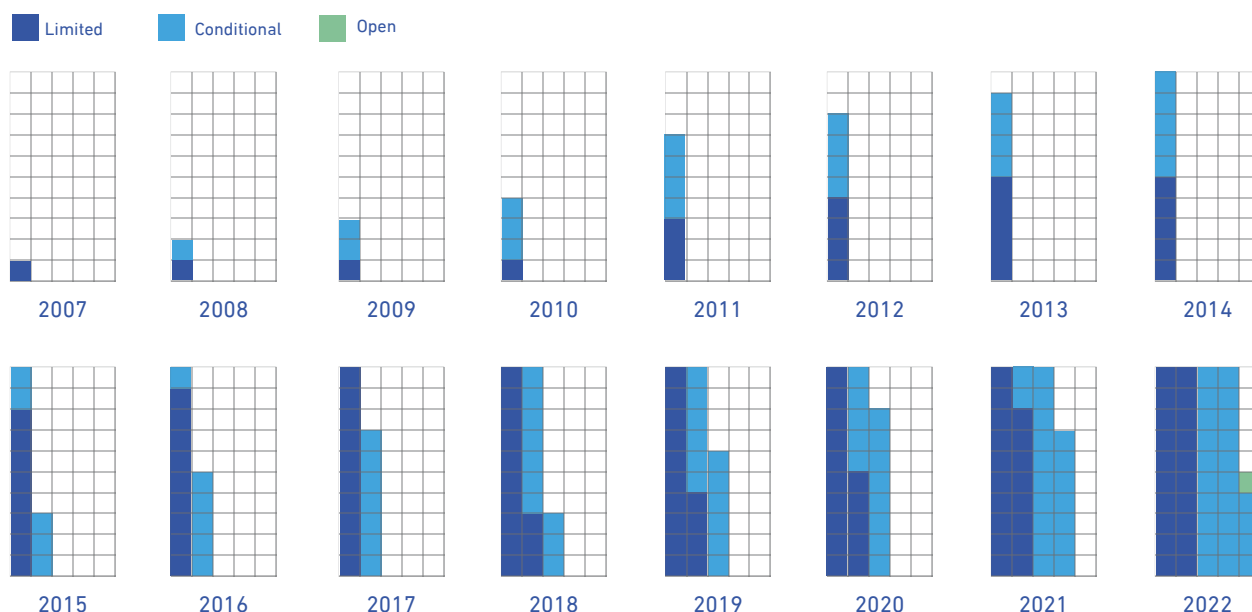


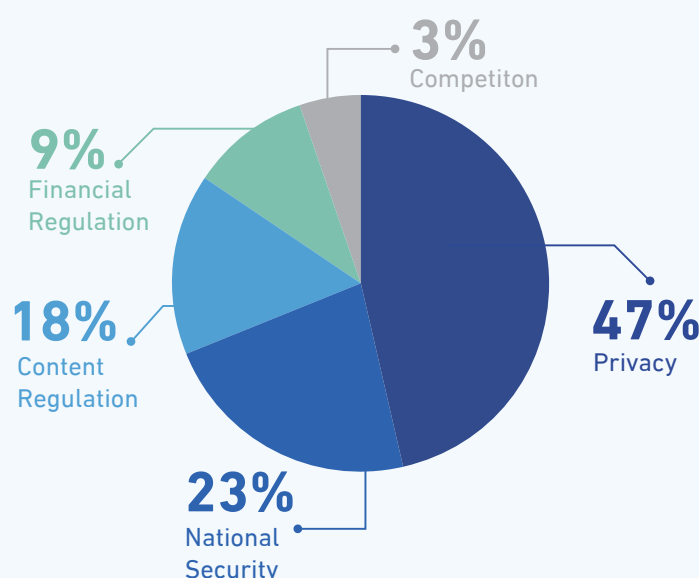
Figure 2: Changes in Data Flow Models Over Time

Figure 02 shows that the growth in data flow regulations has been primarily in the use of the conditional and limited transfer models. The exception is Oman's data protection regulation which is an open transfers model with its largely consent-based mechanism before personal data is able to be exported.

## The Key Drivers of Data Flow Restrictions

There are a range of motivations amongst the DCO Member States that are driving data governance regulation. As can be seen in Figure 03, 47 percent of the data regulation (27 regulations) is about privacy protection, followed by national security, content regulation, financial regulation and then competition.

Figure 03: Cumulative Regulatory Objectives of Cross-Border Data Flows Restrictions



## Interoperability and Cross-Border Data Flows

Interoperability mechanisms enable cross-border data flows while respecting differences in national data governance regulation. Interoperability is not premised on harmonization of data governance regulation while assuming that global alignment on data governance laws and regulations is unlikely. Interoperability can be developed regionally, amongst a group of nations with common interests, or bilaterally.

### There are two main types of interoperability mechanisms:

1. Unilateral recognition of another country's regulation as equivalent in effect, allowing data to flow freely to that country.
2. Mutual recognition of equivalence where both countries agree to recognize each other's regimes as equivalent.



### Developing interoperability mechanisms have three elements:

1. Agreeing on common principles whether with respect to privacy, financial payments or consumer protection.
2. Agreeing on a data classification scheme that will guide regulation and inform the entities holding data.
3. Establish cross-border institutional mechanisms that support interoperability.

The following diagram outlines the key elements of an interoperability mechanism that can support data free flow with trust.

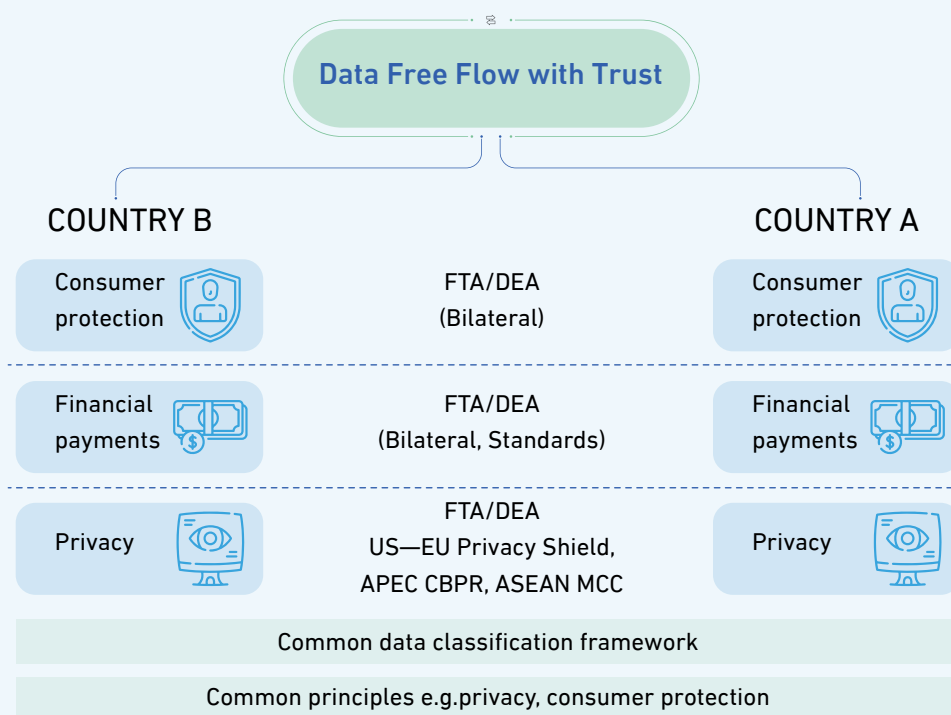


Figure 04: The Building Blocks of Interoperability

## A Data Classification Scheme Amongst DCO Member States

Various countries are considering data classification systems to manage risk from different categories of data, which can help design risk-based approaches to cross-border data flows. The basic distinction being drawn in early data classification efforts have been between personal and non-personal data, with different regimes for each category. For example, the EU takes this approach with the GDPR applying to personal data and the EU Regulation on a framework for the Free Flow of Non-Personal Data in the European Union.<sup>51</sup> The World Bank also advocates a distinction between personal and non-personal data with different regulatory approaches for each one.<sup>52</sup>

Data classification is now extending beyond the binary personal/non-personal to include data that is sensitive — which can be a particular category of personal data used to identify traits such as philosophical and religious beliefs or political preferences. Data classification is also distinguishing critical data that might be sensitive from a national security perspective. Figure 05 shows these data categories and their areas of overlap.

Many of these data classifications are already being used by the DCO Member States. For example, Kuwait, Oman, Saudi Arabia,<sup>53-54</sup> Pakistan, Rwanda, Bahrain and Nigeria distinguish between personal data and critical data in various data regulations. The EU GDPR distinguishes personal data relating to an “identified or identifiable living individual”<sup>55</sup> from sensitive personal

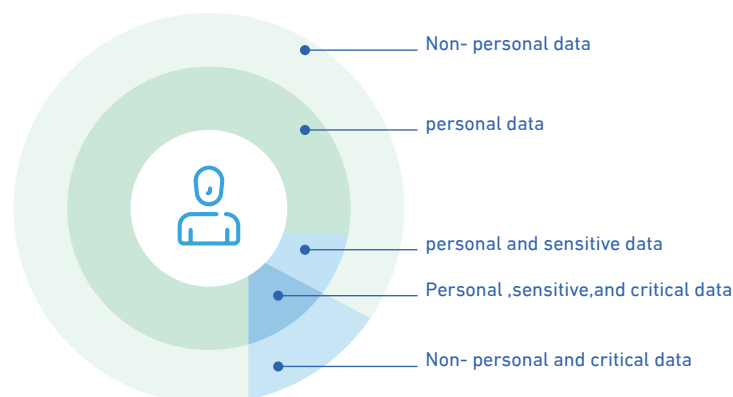


Figure 05: Data Classification

information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs,” to name a few.<sup>56</sup> Data classification is likely to proliferate and form the basis for different regulatory approaches. The implications for data flows will vary, as restrictions on cross-border sensitive personal data will increase, while there will be more free flow allowed for non-personal data that does not pose any national security concerns. DCO Member States should therefore develop a common taxonomy of data classifications, which would help identify opportunities for interoperability. For instance, agreement on what is sensitive personal data would shift the conversation to how to protect that data while also allowing data in other categories to flow.

## Developing Interoperability Mechanisms for Personal Data

Analysis of DCO Member State regulations shows the overwhelming importance of privacy as a driver of data flow regulation. Moreover, and as discussed, the importance of access to personal data for business operations, innovation and government services makes clear the importance of developing interoperability mechanisms to facilitate cross-border flows of personal data. There are several interoperability mechanisms being developed that enable cross-border transfers of personal data which can guide work by DCO Member States.

Key privacy interoperability mechanisms are those under GDPR —specifically adequacy findings, binding corporate rules (BCR) and standard contractual clauses (SCC). APEC Cross-Border Privacy Rules (CBPR) is another interoperability mechanism as is the ASEAN model contractual clauses (MCC) and the US-EU Privacy Shield 2.0.

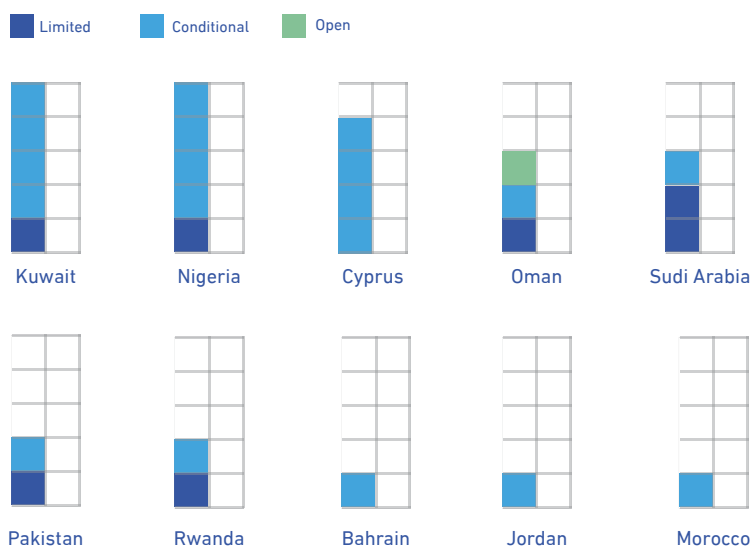


Figure 06: Privacy Regulation by Country and Data Transfer Model

The following table outlines these global privacy interoperability mechanisms as well as their main similarities and differences.

TABLE 02: Main Privacy Interoperability Mechanisms

	GDPR - Adequacy, BCR & SCC	US-EU Privacy Shield 2.0	APEC CBPR	ASEAN Model Contractual Clauses
LEGAL FORCE	Binding	Binding	Voluntary	Voluntary
GROUNDS FOR CROSS-BORDER DATA TRANSFER	<p>The receiving country has:</p> <ul style="list-style-type: none"> <li>• An adequacy decision where the privacy regime is essentially equivalent.</li> <li>• BCRs</li> <li>• SCCs</li> </ul>	<p>Opt-in mechanism. No changes to US privacy law with additional safeguards for EU personal data.</p>	<p>Certification that the receiving entity's privacy policies provide protection consistent with APEC Privacy Rules.</p>	<p>Template terms to include in contracts between entities in ASEAN Member States to ensure data flows are protected and consistent with ASEAN Privacy Framework.</p>
OVERSIGHT BODY	<ul style="list-style-type: none"> <li>• EU Commission assesses and grants adequacy.</li> <li>• EU Data Protection Authorities approve BCRs and SCCs.</li> </ul>	<p>Oversight and enforcement by the United States Federal Trade Commission.</p>	<p>Domestic Accountability Agents certify compliance with privacy policies. APEC Cross-border Privacy Enforcement Arrangement (CPEA) creates a framework for regional cooperation in the enforcement of Privacy Laws.</p>	<p>None</p>
THE ROLE OF INDUSTRY IN ALLOWING DATA FLOW	<ul style="list-style-type: none"> <li>• None for adequacy</li> <li>• Responsible for ensuring compliance with SCC or BCR.</li> </ul>	<p>Responsible for ensuring compliance with privacy policies.</p>	<p>Responsible for ensuring compliance with privacy policies.</p>	<p>Ensuring compliance with MCC terms in the contract.</p>



## Different approaches to Interoperability for Cross-Border Flow of Personal Data

There are a range of ways to develop interoperability mechanisms for personal data amongst the DCO Member States. The interoperability mechanisms could be bilateral, regional or amongst the DCO Member States. As Cyprus is part of the EU, a privacy interoperability mechanism that includes Cyprus will have to be GDPR consistent. This means that an adequacy decision can only be made by the European Commission and BCRs and SCCs will need to be certified by the EU data protection authorities. So far, none of the DCO Member States have obtained such an adequacy finding from the European Commission. The following outlines a multi-step approach to building interoperability of privacy frameworks:



- 1. Agree on privacy principles.** There is already common ground amongst many of DCO Member States whose privacy laws are built on OECD Privacy Principles and have been influenced by GDPR. A common baseline of privacy principles would enable various interoperability mechanisms that will allow data flow.
- 2. Agree on a data classification scheme for personal data:** A data classification scheme that reflects agreement as to what constitutes personal data and sensitive data — the two main ways that the DCO Member States distinguish forms of personal data — would support interoperability and guide entities collecting data on how to best categorize personal data.

**3. Agree on conditions under which data can flow:** There are various approaches that could be adopted to develop interoperability which can be tailored to each country's approach to privacy:

a.

DCO Member States should articulate what is required for an adequacy finding. Many DCO Member States require adequacy before personal data can flow across borders, yet what is required for adequacy is often not well defined. Broadly, there are two options

- i. Follow the EU approach which has defined adequacy strictly as meaning essentially equivalent,
- ii. Provide more flexibility in defining what constitutes adequacy in third countries.

b.

Where adequacy is required in the country receiving the personal data, each DCO Member State should assess whether any of the DCO Member State privacy regulations are adequate. The DCO Member States should assess the likelihood of successfully getting an adequacy finding from the European Commission to enable flows of personal data between Cyprus and other DCO Members, as well as assess the validity of BCRs and SCCs. Separately, DCO Members should develop an everyone but EU (currently Cyprus) strategy for enabling flows of personal data that is more flexible than GDPR.

c.

One option for a flexible interoperability mechanism would be a government-led scheme that businesses in DCO Member States could opt-into, supported by third party oversight of compliance. Participation in the scheme would guarantee that privacy protection was consistent with any agreed upon DCO privacy principles or with other DCO Member States privacy regulation.

d.

DCO Member States could also certify businesses that demonstrate that they follow privacy policies consistent with DCO's commonly agreed privacy principles. Entities in countries requiring adequacy before exporting personal data would be able to send personal data to certified businesses in other DCO countries.

e.

DCO Member States could also develop common standard contractual clauses that when included in contracts would ensure standards of privacy protection consistent with common privacy principles or DCO Member State privacy regulations, enabling cross-border data flows.

## Supporting Cross Border Payments

Cross-border payments rely on exchange of data to work. Enabling cross-border payments at the retail and wholesale levels can reduce costs of international e-commerce, expand opportunities for businesses to participate in cross-border digital trade and improve flows of remittances. As outlined, financial regulation is an important reason for data flow restrictions amongst the DCO



Member States. This includes Pakistan's State Bank Regulations, which restricts international transfers of consumer transactions at banks, Nigeria's data requirements for its Central Bank which require local storage and processing for entities dealing in point-of-sale card services, and Kuwait's Cybersecurity Framework for its banking sector, which requires appropriate data protection and privacy measures. Yet, cross-border payments often experience delays and greater costs when compared with domestic payments. There are a range of regulations and standards related to cross-border payments that create costs and delay.

Interlinking payments systems to enable more efficient cross-border payments which will require data flows of financial information. New technologies, increasing standardization and application programming interfaces (APIs) can also enhance interoperability of cross-border payments.

## Electronic Payment



**In 2020, the G20 endorsed a roadmap to enhance cross-border payments. There are a range of steps DCO Member States could take to promote interoperability and the interlinking of electronic payment infrastructures:**

- a. Modernize the regulation on consumer protection, privacy and financial sector to achieve trust and security that is predictable and appropriate to the risks posed by the provision of electronic payment services.
- b. Encourage innovation and competition in electronic payments services.
- c. Make publicly available regulations on electronic payments, including in relation to regulatory approvals, licensing requirements, procedures and technical standards.
- d. Avoid arbitrarily or unjustifiably discriminating between financial institutions and non-financial institutions in relation to access to services and infrastructure necessary for the operation of electronic payment systems.
- e. Adopt, for relevant electronic payment systems, international standards for electronic payment messaging, such as the ISO 20022 Universal Financial Industry Message Scheme, for electronic data exchange between financial institutions and services suppliers to enable greater interoperability between electronic payment systems.
- f. Facilitate the use of open platforms and architectures such as tools and protocols provided for through APIs and encourage payment service providers to safely and securely make APIs for their products and services available to third parties, where possible, to facilitate greater interoperability, innovation and competition in electronic payments.



## Developing Cross-Border Digital IDs

Another related area that can facilitate cross-border digital payments would be to develop domestic digital IDs and the mutual recognition of digital IDs across borders. Countries could also consider bilateral or multilateral agreements on digital IDs.

**Steps that DCO Member States could take include:**

a.

Modernize the regulation on consumer protection, privacy and financial sector to achieve trust and security that is predictable and appropriate to the risks posed by the provision of electronic payment services.

b.

Establishing frameworks to foster technical interoperability or common standards between each DCO Member State on digital identities.

c.

Providing comparable protection of digital identities afforded by each DCO Member State's respective legal frameworks, or the recognition of their legal and regulatory effects, whether accorded autonomously or by mutual agreement.

d.

Agreeing to exchange knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and user adoption.



## Glossary and Abbreviations

<b>APEC CBPR</b>	Asia Pacific Economic Cooperation Cross-Border Privacy Rules
<b>APEC PEA</b>	Asia Pacific Economic Cooperation Privacy Enforcement Authorities
<b>ASEAN MCC</b>	Association of Southeast Asian Nations Model Contractual Clauses
<b>BCRs</b>	Binding Corporate Rules
<b>CJEU</b>	Court of Justice of the European Union
<b>CNDP</b>	Morocco's National Commission for the Protection of Personal Data Protection
<b>CPTPP</b>	Comprehensive and Progressive Trans-Pacific Partnership
<b>DEA</b>	Digital Economy Agreement
<b>DFFT</b>	Cross-Border Data Free Flow with Trust: Concept of a global digital environment that enables the movement of data across international borders while ensuring that, upon crossing a border, data are granted the desired oversight and protection (OECD)
<b>EU GDPR</b>	European Union General Data Protection Regulation
<b>FTA</b>	Free Trade Agreement
<b>G7 Digital Trade Principles</b>	Data should be able to flow freely across borders with trust
<b>ID4D</b>	Nigeria's Digital Identification for Development program
<b>ISO 20022</b>	International Organization for Standardization (ISO) 20022 Universal Financial Message Scheme messaging standards
<b>Malabo Convention</b>	African Union Convention on Cyber Security and Personal Data Protection 2014
<b>NAFTA</b>	North American Free Trade Agreement
<b>OECD Guidelines</b>	Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Trans-Border Flows Personal Data
<b>PSP</b>	Payment System Provider
<b>RECP</b>	Regional Comprehensive Economic Partnership
<b>Schrems II</b>	Ruling of the CJEU affecting businesses transferring personal data outside of European Economic Area
<b>SCCs</b>	Standard Contractual Clauses Total Factor Productivity - The degree of operational efficiency of a business that measures how much output can be produced from a certain amount of inputs.
<b>USITC</b>	United States International Trade Commission
<b>USMCA</b>	United States-Mexico-Canada Agreement
<b>US-EU Privacy Shield 2.0</b>	The Trans-Atlantic Data Privacy Framework
<b>WTO GATS</b>	World Trade Organization General Agreement on Trade in Services

This report is a working paper, and hence it represents research in progress. It is the product of professional research by the DCO in collaboration with the firm Policyware. It was produced as a collaboration to facilitate public debate in the DCO Member States. It is published under the responsibility of the Secretary-General of the DCO and the Policyware firm. It does not necessarily reflect the official views of the DCO Member States, nor the official position of any of DCO staff members. The information herein may not be exhaustive or accurate. The names of companies, entities, products, services, etc. mentioned in this document are not intended as an endorsement or referral to by the DCO, its Member States or staff members. They are not sorted in the order of preference.

© 2023 DIGITAL COOPERATION ORGANIZATION. All rights reserved.

## About the Digital Cooperation Organization



The DCO is a global Intergovernmental Organization founded in November 2020 that aims to enable digital prosperity for all by accelerating the inclusive and sustainable growth of the digital economy. The DCO is focused on empowering youth, women, and entrepreneurs, leveraging the accelerative power of the digital economy and leapfrogging with innovation to drive economic growth and increase social prosperity. Through enhanced cooperation and dialogue, the DCO seeks to establish a conducive environment for the rapid development of digital economies within which all individuals, businesses and societies can innovate and thrive.

In pursuit of its purpose, the DCO fosters multilateral collaborations across sectors to allow governments, private sector, international organizations, and civil society to cocreate, and codesign initiatives that enable more inclusive digital transformation and the growth of digital industries. The DCO's main flagship interventions include programs and initiatives that aim to enhance cross-border data flows, market access for SMEs, digital entrepreneurs' empowerment, digital taxation, and digital inclusion.

## About Policyware



**policyware**

Policyware provides online deep dives into the most pressing public policy issues. Each Deep Dive is curated, concise and designed by experts from the top universities and think tanks globally to provide the tools, information, and insights needed to understand the issues to develop new and innovative policy solutions to the most pressing challenges. Policyware also provides bespoke training and analysis on cutting-edge public policy topics. Current Policyware Deep Dives include: global developments affecting digital trade and data flows, understanding China's digital governance regime, the latest developments in international investment policy, how climate change is driving international trade and investment policy, global experience financing ESG outcomes including impact bonds, global developments in privacy law and policy, developments in AI regulation and R&D, and a deep dive into export controls in the US and key economies and what comes next.

## CONTRIBUTORS

We would like to express our gratitude to all of those with whom we have had the pleasure to work on this paper. The larger contributing team includes:

### AUTHORS

**Joshua Meltzer** (Lead Author)  
CEO  
**Policyware**  
[www.policyware.org](http://www.policyware.org)

**Ahmad Bhinder**  
Policy Innovation Director  
**DCO**

### ACKNOWLEDGEMENTS

**Alaa Abdulaal**  
Chief of Digital Economy Foresight  
**DCO**

**Hassan Nasser**  
Chief of Cabinet  
**DCO**

**Khaldoon Said**  
Marketing & Communications Director  
**DCO**

**Khalid Abu Awad**  
PMO Director  
**DCO**

**Manal Bondi**  
Acting Chief of Digital Markets Growth  
**DCO**

## Bibliography

1. 2019 Osaka G20 Leader's Declaration, [https://www.mofa.go.jp/policy/economy/g20\\_summit/osaka19/en/documents/final\\_g20\\_osaka\\_leaders\\_declaration.html](https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html)
2. "Digital Economy," Government, bahrain.bh, accessed December 15, 2022, <https://www.bahrain.bh/wps/portal/en/BNP/About-TheKingdom/DigitalEconomy>
3. GlobalData, media article Jul 2022, <https://www.globaldata.com/store/report/bahrain-ict-market-analysis/#:~:text=The%20global%20ICT%20market%20in%20Bahrain%20size%20was%20estimated%20at,US%244.6%20billion%20in%202022.>
4. Digital Cyprus Strategy 2020-2025, [https://www.dmrid.gov.cy/dmrid/research.nsf/all/927EA351714F99EDC22587CE-0028C090/\\$file/Digital%20Strategy%202020-2025.pdf?openelement](https://www.dmrid.gov.cy/dmrid/research.nsf/all/927EA351714F99EDC22587CE-0028C090/$file/Digital%20Strategy%202020-2025.pdf?openelement)
5. <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/cyprus-national-digital-strategy-2020-2025>
6. <https://www.jordanvision.jo/en>
7. Jordan's Digital Future: A Conversation with Jordanian Minister of Digital Economy and Entrepreneurship, July 29, 2021, <https://www.wilsoncenter.org/event/jordans-digital-future-conversation-jordanian-minister-digital-economy-and-entrepreneurship>
8. Kuwait National Development Plan 2020-2025, [https://media.gov.kw/assets/img/Ommah22\\_Awareness/PDF/NewKuwait/Revised%20KNDP%20-%20EN.pdf](https://media.gov.kw/assets/img/Ommah22_Awareness/PDF/NewKuwait/Revised%20KNDP%20-%20EN.pdf)
9. [https://add.gov.ma/storage/pdf/Avril\\_NOG\\_ADD\\_fr\\_SITE\\_VF.pdf](https://add.gov.ma/storage/pdf/Avril_NOG_ADD_fr_SITE_VF.pdf)
10. <https://www.bmz-digital.global/en/initiatives/digital-transformation-center-morocco/>
11. <https://www.add.gov.ma/presentation-de-ladd>
12. Nigeria Digital Economy Development Department, <https://nitda.gov.ng/department/the-digital-economy-development-department/>
13. Oman Digital Transformation [https://oman-portal.gov.om/wps/portal/index/etransformationplan/!ut/p/a1/04\\_Sj9CPyKssy0xPLMn-Mz0vMAfGjzOL9Aw3NDD38DbwtDlydDRydn-P1NTAwdDfxDjYAKloEKDHAARwNC-sP1o8B-KjA3cDQz8LT19vUN8HQ2MjMPcvCx9zIx-dXEygCvBYEYap1-QG2GQZeKoCADwbFGg/dl5/d5/L0IKQSEvUUt3RS80RUkhL2Vu/](https://oman-portal.gov.om/wps/portal/index/etransformationplan/!ut/p/a1/04_Sj9CPyKssy0xPLMn-Mz0vMAfGjzOL9Aw3NDD38DbwtDlydDRydn-P1NTAwdDfxDjYAKloEKDHAARwNC-sP1o8B-KjA3cDQz8LT19vUN8HQ2MjMPcvCx9zIx-dXEygCvBYEYap1-QG2GQZeKoCADwbFGg/dl5/d5/L0IKQSEvUUt3RS80RUkhL2Vu/)
14. Oman Vision 2040 [https://www.mof.gov.om/pdf/Vision\\_Documents\\_En.pdf](https://www.mof.gov.om/pdf/Vision_Documents_En.pdf)
15. GlobalData, Mar 2020, <https://www.globaldata.com/media/technology/ict-spending-in-oman-will-reach-us5-6bn-in-2024/>
16. Digital Pakistan Policy, Ministry of IT and Telecom, [http://moib.gov.pk/Downloads/Policy/DIGITAL\\_PAKISTAN\\_POLICY%2822-05-2018%29.pdf](http://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf)
17. "Unlocking Pakistan's Digital Potential" Alpha-Beta, October 2021: <https://alphabeta.com/wp-content/uploads/2021/10/pakistan-digital-transformation.pdf>
18. [https://www.minecofin.gov.rw/fileadmin/user\\_upload/Minecofin/Publications/REPORTS/National\\_Development\\_Planning\\_and\\_Research/Vision\\_2050/English-Vision\\_2050\\_Abridged\\_version\\_WEB\\_Final.pdf](https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Publications/REPORTS/National_Development_Planning_and_Research/Vision_2050/English-Vision_2050_Abridged_version_WEB_Final.pdf)
19. <https://www.bloomberg.com/news/articles/2022-04-12/rwanda-looks-to-space-to-boost-information-technology-footprint?leadSource=verify%20wall>
20. [https://www.nirda.gov.rw/uploads/tx\\_dce/National\\_Strategy\\_For\\_Trsansformation\\_NST1-min.pdf](https://www.nirda.gov.rw/uploads/tx_dce/National_Strategy_For_Trsansformation_NST1-min.pdf)
21. Digital Economy Policy in the Kingdom of Saudi Arabia, [https://www.mcit.gov.sa/sites/default/files/digitaleconomypolicy\\_en.pdf](https://www.mcit.gov.sa/sites/default/files/digitaleconomypolicy_en.pdf)
22. <https://focusonbusiness.eu/en/education/ict-spending-in-saudi-arabia-will-reach-us-46-6bn-by-2023/3446#:~:text=2%20min.,leading%20data%20and%20analytics%20company.>

23. <https://smex.org/wp-content/uploads/2021/12/The-Digital-ID-Landscape-In-the-GCC-1.pdf>
24. <https://www.idemia.com/news/kingdom-morocco-launches-national-digital-id-platform-idemia-2022-05-19>
25. Stefano Kelelis, "Introduction of the Electronic Identity Card in Cyprus," Cyprus Mail (blog), June 1, 2022, <https://cyprus-mail.com/2022/06/01/introduction-of-the-electronic-identity-card-in-cyprus/>.
26. Frank Hersey, "Digital ID Status Update for Nigeria and Rwanda: New Technology, Data Law | Biometric Update," Biometric Update, September 16, 2022, <https://www.biometricupdate.com/202109/digital-id-status-update-for-nigeria-and-rwanda-new-technology-data-law>.
27. "Jordan ID: A New National ID Card Program," Thale, accessed December 16, 2022, <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/national-id-card-jordan>.
28. Jim Nash, "National Digital ID Issuance for Pakistanis Ramping Up," Biometric Update, August 26, 2022, <https://www.biometricupdate.com/202208/national-digital-id-issuance-for-pakistanis-ramping-up>.
29. Macdonald, "Nigeria Reaches 90M Digital ID Registrations as Database Capacity Issue Looms."
30. Burt, "Nigeria's Digital ID Strides Hailed, but More Work Needed to Hit 148M Enrollments by 2024."
31. <https://martechvibe.com/article/bahrain-and-ksa-may-integrate-digital-id-verification-system/>
32. Developing the Implementation Approach for the Cross-Border Payments Targets, Final Repot, Financial Stability Board, 17 November 2022 <https://www.fsb.org/wp-content/uploads/P171122.pdf>
33. OECD, OECD Digital Economy Outlook 2020 (OECD, 2020), <https://doi.org/10.1787/bb167041-en>.
34. McKinsey Global Institute, "Global flows: The ties that bind in an interconnected world", Discussion Paper, November 15, 2022 <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world>
35. UNCTAD "Digitalisation of Services: What Does It Imply To Trade and Development? UNCTAD 2022
36. Louis Dron et al, "Data capture and sharing in the COVID-19 pandemic: a cause for concern", The Lancet ,October 2022, [https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(22\)00147-9/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00147-9/fulltext)
37. Bertin Martens, "The impact of data access regimes on artificial intelligence and machine learning," JRC Digital Economy Working Paper 2018–19, EU Science Hub,[https://joint-research-centre.ec.europa.eu/publications/impact-data-access-regimes-artificial-intelligence-and-machine-learning\\_en](https://joint-research-centre.ec.europa.eu/publications/impact-data-access-regimes-artificial-intelligence-and-machine-learning_en)
38. "How AI Can Pump New Life into Oilfields," Expert Insights (IBM, February 2020), <https://www.ibm.com/downloads/cas/5BNKGNLE>.
39. OECD, Mapping Approaches to Data and Data Flows, Report for the g20 Digital Economy Task Force, Saudi Arabia, <https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf>
40. Small Online Business Growth Report, ebay <https://static.ebayinc.com/static/assets/Uploads/PressRoom/Local/Imported/Small%20Online%20Business%20Growth%20Report.pdf>
41. World Bank, World Development Report 2021: Data for Better Lives (The World Bank, 2021), [https://doi.org/10.1596/978-1-4648-1600-0\\_p.13-14](https://doi.org/10.1596/978-1-4648-1600-0_p.13-14).
42. World Bank, World Development Report 2021: Data for Better Lives (The World Bank, 2021), <https://doi.org/10.1596/978-1-4648-1600-0>.
43. Erik van der Marel, Hosuk Lee-Makiyama, and Matthias Bauer, "The Costs of Data Localisation: A Friendly Fire on Economic Recovery," EPICE, May 2014, <https://ecipe.org/publications/dataloc/>.



44. Nigel Corey and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Foundation, July 19, 2021, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>
45. Nigel Corey and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Foundation, July 19, 2021, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>
46. Martina F. Ferracane and Erik van der Marel, "The Cost of Data Protectionism," EPICE, October 2018, <https://ecipe.org/blog/the-cost-of-data-protectionism/#ftnref7>
47. Martina F. Ferracane and Erik van der Marel, "The Cost of Data Protectionism," EPICE, October 2018, [https://ecipe.org/blog/the-cost-of-data-protectionism/#\\_ftnref7](https://ecipe.org/blog/the-cost-of-data-protectionism/#_ftnref7)
48. Quantifying the Cost of Forced Localization, Leviathan Security Group, accessed December 16, 2022, <https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization>
49. Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year," Center for Data Innovation (blog), June 17, 2019, <https://datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>
50. Kati Suominen and Erica Vambell, "Alliance for E-Trade Development: Toward an African Data Transfer Regime to Enable MSMEs' Cross-Border E-Commerce" (US-AID Center for Economics and Market Development), accessed December 15, 2022, [https://www.allianceforetradedevelopment.org/files/ugd/478c1a\\_72021e35a826441db0723642a79e65e5.pdf](https://www.allianceforetradedevelopment.org/files/ugd/478c1a_72021e35a826441db0723642a79e65e5.pdf). Mona Farid Badran and Rizwan Tufail, "Economic Impact of Data Localization in 5 Selected African Countries, an Empirical Study," accessed December 15, 2022, [https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC\\_RANITP\\_Economic\\_Impact\\_of\\_Data\\_Localization\\_in\\_5\\_selected\\_African\\_Countries.pdf](https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf)
51. REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, L303/59, <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in-%20Europe>
52. World Bank Development Report 2021, p 190, <https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1600-0>
53. "Saudi Arabia Releases Version 3 of Its Cloud Computing Regulatory Framework | DLA Piper," DLA Piper, April 27, 2021, <https://www.dlapiper.com/en-om/insights/publications/2021/04/saudi-arabia-releases-version-3-of-its-cloud-computing-regulatory-framework>
54. <https://sdaia.gov.sa/ndmo/Files/PoliciesEn001.pdf>
55. "What Is Personal Data?," European Commission, accessed December 16, 2022, [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)
56. "What Personal Data Is Considered Sensitive?," European Commission, accessed December 16, 2022, [https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en)



Follow Us on

   @dcorg |  [www.dco.org](http://www.dco.org)