

Enabling Cross-Border Data Flows Amongst the Digital Cooperation Organization Member States

October 2023



FOREWORD



I commend the General Secretariat of the Digital Cooperation Organization on the successful completion of this report which provides a comprehensive analysis of data governance regulations impacting cross-border data flows across the Organization's Member States.

Accessing and using data becomes critical as we progress into the digital economy. This report highlights the significant growth in data governance regulations and emphasizes the need to balance the opportunities of cross-border data flows with safeguarding privacy, consumer protection, and national security. To achieve this balance, we need the right interoperability mechanisms, and we can develop these as suited for our people by taking inspiration from others as well as having a comparative understanding of different frameworks such as US-EU Privacy Shield 2.0, APEC Cross-Border Privacy Rules, and the ASEAN Model Contractual Clauses. Enabling cross-border data flows is a priority area for the DCO. The flow of data underpins many of our other initiatives, such as empowering SMEs to work across-borders and attracting digital foreign direct investment. As the President of the Council of the DCO, I look forward to more DCO initiatives to support increased cooperation and interoperability between our Member States to maximize the benefits of the cross-border flow of data with trust.

As with most challenges we face due to our transforming industries, governments, and businesses, the key to ensuring we are all equally equipped to leverage the opportunities in the digital economy lies in cooperation, knowledge transfer, and exchange of best practices. With the insightful analysis herein, this report will serve as a source of inspiration and a useful guide for other nations as they develop effective data governance regulations that enable data free flows with trust.

H.E. Mr. Mohamed bin Thamer Al Kaabi

Chairperson, Digital Cooperation Organization

Minister of Transportation and Telecommunications, Kingdom of Bahrain

FOREWORD




Data is the fuel of future global economic expansion. An estimated 70% of new value created in the economy over the next decade will be based on digitally enabled platform business models. Global digital economy is dependent on accelerating digital transformation and on cross-border data flows.

The digital economy provides an abundance of opportunities for all nations and all social groups, and for these opportunities to be harnessed, nations of the world must come together to efficiently cooperate to exchange data across borders while preserving national data sovereignty and individuals' data privacy. This requires innovative multilateral and multi-stakeholder cooperation models.

Data regulations are undoubtedly essential to preserve individual privacy, protect national security, uphold regulations in finance and healthcare, and support other governmental requirements. Many nations today have some form of data legislation to provide protection and controls on sensitive information. However, in many instances, legitimate data regulations have hindered the growth of cross-border data flows. According to an economic model developed by the Information Technology and Innovation Foundation, increases in Data restrictiveness can impact a nation's domestic and global economy by decreasing trade volume and productivity while increasing prices.

The challenge for nations is finding a balance between maximizing the opportunities from cross-border data flows while respecting data privacy and consumer protection and preserving national data sovereignty. In this report, the DCO takes a closer look at how nations of the world can achieve a workable balance between data protection and the free flow of data; and develop the frameworks and mechanisms that will allow us to achieve effective, trusted means of data exchange that transcend our borders.



In addition to the aforementioned challenges, nations may also face the challenges of data governance, modeling, interoperability, and data commercialization.

Many nations already have data laws in place or under development, and their right to preserve data must be respected. Creating alignment between them on a harmonized set of data regulations would be difficult. But by working together in a spirit of cooperation, nations can demonstrate how governments can use common data principles and classifications, and mutual transparency, to create mechanisms for trusted and fair interoperability between data governance regimes. We can develop the means for cross-border data flows with trust while respecting the autonomy of nations to implement their own data laws.

By showing how nations of the world can solve the challenge of cross-border data flows, we demonstrate how they can drive their digital economies, enhance trade, and enable prosperity for all. The Digital Cooperation Organization enables nations to accelerate the growth of a global inclusive, sustainable, and thriving digital economy.

Deemah AlYahya
Secretary-General
The Digital Cooperation Organization

TABLE OF CONTENTS

Executive Summary	07
Part 1: The Economic and Trade Opportunities from Data	09
DCO Member States are Building their Digital Economies	10
Assessing the Opportunities from Cross-Border Data Flows	14
The Costs of Limits to Cross-Border Data Flows	16
The Different Cross-Border Data Flow Models	20
Part 2: Regulating for a Growing Digital Economy	21
Regulations Affecting Data Flows Amongst the DCO Member States	22
The Key Drivers of Data Flow Restrictions	23
Part 3: Enabling Cross-Border Data Flows and Regulation	25
Getting to the G20 Goal of Data-Free Flows with Trust	26
Interoperability and Cross-Border Data Flows	27
Interoperability in Trade Agreements and Digital Trade Agreements	28
Developing Interoperability Mechanisms	30
Agree on a Data Classification Scheme	32
Part 4: Developing Interoperability Mechanisms	35
Privacy Regulation and Cross-Border Data Flows	36
Existing Privacy Interoperability Mechanisms	37
Developing Interoperability for Cross-Border Flow of Personal Data	42
Supporting Cross Border Payments	44
Developing Cross-Border Digital IDs	47
Part 5: Conclusion	49
Glossary and Abbreviations	51
Bibliography	54

TABLE OF FIGURES

Figure 01. Cumulative Growth in Number of Cross-Border Data Flow Regulations	22
Figure 02. Changes in Data Flow Models Over Time	22
Figure 03. Data Transfer Models by Country	23
Figure 04. Cumulative Regulatory Objectives of Data Governance Regulations that Affect Cross-Border Data Flows	23
Figure 05. Number of Data Regulations by Regulatory Objective Over Time	24
Figure 06. Key Digital Trade Commitments in Major Trade Agreements	28
Figure 07. The Building Blocks of Interoperability	31
Figure 08. Data Classification	33
Figure 09. Privacy Regulation by Country and Data Transfer Model	36

Purpose of the report

The purpose of this report is to provide an understanding of the regulatory frameworks that affect cross-border data flows amongst ten Member States of the DCO: Bahrain, Cyprus, Jordan, Kuwait, Morocco, Nigeria, Oman, Pakistan, Rwanda, and Saudi Arabia. The report provides recommendations on how to develop interoperability mechanisms to enable cross-border flows of data with trust amongst the DCO Members States. Although the report includes analysis from the ten mentioned DCO Member States, it contains valuable insights and recommendations for all DCO membership and beyond.

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.

The 2019 Osaka G20 established the goal of Data Free Flow with Trust (DFFT) - a goal reflected in all subsequent G20 and G7 Statements. Various trade agreements and digital economy agreements support data free flows with trust with commitments to cross-border data flows as well as the commitment to having laws that protect the privacy of and provide consumer protection.

This report provides a detailed overview of the data governance regulations of 10 Member States of the Digital Cooperation Organization (DCO) — Kingdom of Bahrain, Republic of Cyprus, Hashemite Kingdom of Jordan, State of Kuwait, Kingdom of Morocco, Federal Republic of Nigeria, Sultanate of Oman, Islamic Republic of Pakistan, Republic of Rwanda, and Kingdom of Saudi Arabia.

In these DCO Member States, in line with the global trend, there has been significant growth in data governance regulations affecting cross-border data flows. Adoption of these regulations has been motivated by various factors, including the protection of personal data, content regulation, financial regulation, and national security.

The growth in data governance regulations highlights a key challenge for the DCO Member States: How to maximize the opportunities from cross-border data flows while also safeguarding privacy, consumer protection, and strengthening national interests. This report analyzes how interoperability mechanisms can maximize access to data and respect regulatory autonomy. Interoperability mechanisms take the domestic regulatory environment largely as given and focus instead on the regional, multilateral, and bilateral arrangements that can enable cross-border data flows.

The importance of interoperability mechanisms for enabling growth in digital economy and digital trade has made developing these mechanisms a priority for many governments and international fora. Significantly, several interoperability mechanisms have been developed, particularly with respect to personal data, that DCO Member States can draw on and learn from to develop their own interoperability mechanisms.

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 enabled by mutual agreement in which arrangements are put in place to support cross-border data flows while also respecting the regulatory differences between countries. The US-EU Privacy Shield 2.0, APEC Cross-Border Privacy Rules, and ASEAN Model Contractual Clauses are examples of interoperability mechanisms.

This report outlines steps that the DCO Member States can take to develop interoperability mechanisms, with a focus on enabling flows of personal data, linking financial payment systems, and cross-border recognition of Digital IDs. In addition, this report recommends that DCO Member States explore ways to 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 the recipient country. This will further support the cross-border data flows.

This report also recommends that DCO Member States develop a common data classification scheme that will support interoperability mechanisms and provide guidance to businesses holding data on how to classify data and understand its risks.

This report proceeds as follows:

Part 1 analyzes the economic and trade opportunities from data for the digital economy and international trade. This part also outlines the economic and business costs from limiting cross-border data flows.

Part 2 analyzes the regulation in ten DCO Member States that affect cross-border data flows and the regulatory goals driving these regulations.

Part 3 discusses key steps to develop interoperability mechanisms, including the agreement on data classification and common data governance principles.

Part 4 discusses specific interoperability mechanisms with a focus on enabling cross-border flows of personal data, as well as cross-border data flows that support linking digital payment systems and digital IDs.

Part 5 concludes.

PART 1: THE ECONOMIC AND TRADE OPPORTUNITIES FROM DATA

DCO Member States are Building Their Digital Economies

DCO Member States are adopting digital transformation programs to achieve economic diversification, create more jobs for women and their young populations, and maximize the opportunities for 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, DCO Member States have developed digital economy policies. For example, **Saudi Arabia's** Vision 2030 is heavily focused on digital transformation that includes developing its digital infrastructure, improving the quality and use of data, and expanding the use of emerging technologies¹.

In fact, ICT spending in Saudi Arabia is forecast to grow at an annual compound rate of



9.2%
between 2019-
2024 and reach
US\$46.6bn.²

Jordan's Modernisation Vision 2022³ 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.

The vision identifies several initiatives to achieve these targets. 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, including expanding the use of Artificial Intelligence⁴.

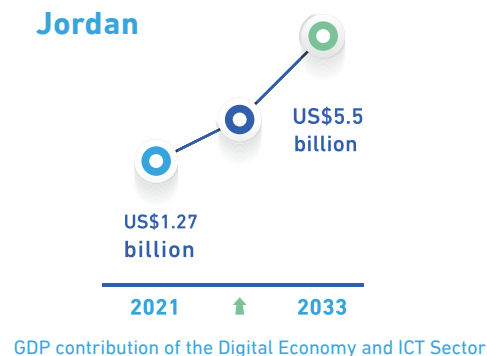
Pakistan is focused on digitization and building a knowledge economy to build on its already world-class IT talent⁵. By one estimate, Pakistan's digital transformation could generate productivity gains, revenue boosts, cost savings, and GDP increments up to PKR9.7 trillion (US\$59.7 billion) worth of economic value annually in Pakistan's economy by 2030⁶.

Kuwait aims to increase broadband speeds and focuses on Smart Cities while also creating an integrated ecosystem for technology, innovation, and knowledge that includes better use of data⁷.

Bahrain aims to be a leading digital economy that includes a focus on cloud computing and ICT infrastructure to support innovation⁸. The Bahrain ICT market was valued at US\$3.81 billion in 2022 and will 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 providers in Bahrain is estimated at US\$ 29.41 billion between 2022 to 2027⁹.

Nigeria's Digital Economy Development Department is focused on supporting the growth of Nigerian digital economy, including improving exchanges of digital goods and services, and increasing the use of digital technologies across the economy¹⁰.

Jordan



Pakistan



Bahrain



Oman is also focused on digital transformation and is using data to improve the efficiency and productivity of the public and private sectors¹¹. In fact, digital transformation initiatives related to Oman Vision 2040¹² are expected to boost the Sultanate's ICT market to OMR 2.2 billion (US\$ 5.6 billion) in 2024¹³.

Cyprus's Digital Strategy 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 competitiveness¹⁴. Cyprus's Recovery and Resilience Plan (RRP) 2021, to be completed by 2026, includes significant investments of around €282 million (US\$ 304.8 million), devoting 23% of the total cost to digital objectives¹⁵.

Morocco aims to position itself as a strong African digital hub. The 'General Guidelines for Development of the Digital in Morocco by 2025'¹⁶ frame digitalization as a strategic lever for development.¹⁷ These guidelines are issued by the Agence de Développement du Digital (Agency for Digital Development) - ADD, which is responsible for implementing Morocco's digital development initiatives and promoting dissemination of digital tools. 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.

Rwanda is making efforts to become a major innovation hotspot in Africa and pushing forward with digital development¹⁸. The government is aiming to triple the representation of its GDP in the technology industry, from current 3% to 10% over the next decade¹⁹. Rwanda's Vision 2050 emphasizes on building a knowledge intensive economy that is driven by data and excels in R&D and innovation²⁰. Furthermore, Rwanda's National Strategy for Transformation (NST1) 2017-2024²¹ includes enhancing digital literacy and increasing the uptake of digital financial services as key strategic interventions to boost digital economy.

The clear message is that the DCO Member States have identified the digital economy as a key opportunity.

Oman



ICT Market

US\$5.6

billion
boost expected
to the Sultanate's
ICT market in
2024

Cyprus



Digital Investments

23%

of the total cost to
digital objectives.

Morocco

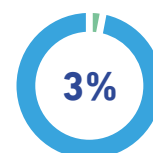


Digital Transformation

15

projects to support the
digital transformation
of Morocco

Rwanda



3%



10%

GDP in the technology industry, from
current 3% to 10% over the next decade

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.

Most DCO Member States have either developed or are in the process of developing digital IDs. This includes Bahrain, Kuwait, Oman, and Saudi Arabia²² in the Gulf, as well as Morocco²³, Cyprus²⁴, Nigeria, Rwanda,²⁵ Jordan²⁶, and Pakistan²⁷.

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^{28 29}. These efforts are underpinned by Nigeria's National Identity Management Commission (NIMC) which is registering all citizens with Unique National Identification Numbers³⁰.

Nigeria



140 million
people
Nigeria Digital
Identification for
Development
(ID4D) project
2024



Bahrain has recently launched a new electronic passport that includes a security chip to store the biometric information of the passport holder.

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 allow Bahraini and Saudi Arabian citizens to access each other's national platforms when visiting their respective countries and would help streamline commercial and investment procedures between the two countries. This should allow users to carry out online transactions using a

digital ID without the need for Bahraini investors to visit Saudi Arabia or vice versa³¹.

Interlinking digital payment systems is another key element 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 completed³². Linking cross-border financial payments can enable e-commerce and have an important development angle.

For instance, increasing access to digital payment services can substitute for credit cards that require bank accounts and 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 Banks and other financial institutions of Bahrain and Kuwait.

Only about ten percent globally of payment systems participate in interlinking arrangements, highlighting the scope for progress.

Assessing the Opportunities from Cross-Border Data Flows



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 globe³³.

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 2019-2021³⁴.



The ability to exchange data across borders is also a key enabler of international trade. For example, to engage in cross-border e-commerce, businesses must collect customer data, and fast and cost-effective digital payments are needed to complete cross-border e-commerce transactions.

In addition, efficient customs and delivery services rely on cross-border data flows to track and trace goods to their destination.

Work by the World Bank has highlighted the role of data flows along supply chains to manage production schedules, respond to changes in consumer demands and track and trace products across global production networks. 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-19³⁵. Access to large data sets remains a key input to developing AI systems, further highlighting the importance of cross-border data flows³⁶.

Collecting data about business operations, customer trends, or suppliers can also yield insights and improve business outcomes. The oil and gas sector is now collecting more data than ever before. Large data sets combined with powerful algorithms are opening new opportunities for this sector.

For example, remote oil and gas operations can be directed from teams located in safe, centralized locations using real-time operational data. Such data-driven insights that use AI-enabled predictions can also reduce operational downtime³⁷.

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. Data is also being used to anticipate customer demands better and to deliver data-driven digital services that add value to traditional goods-only strategies³⁸. Where operations or customers are global, then cross-border data flow will be needed to ensure that these opportunities are applied across the business.

While access to data and global data flows are important for large multinational companies (MNCs), data is also important for small businesses. In fact, many of the opportunities for cross-border data flows are particularly pronounced for small businesses, and the costs of restricting access to data are potentially most impactful on small businesses³⁹. For instance, global data flows allow small businesses access to a global market⁴⁰. This includes access

to global business services inputs that increasingly reside in the cloud, including business software and professional services platforms that provide small businesses with global access to talent.

From a development perspective, access to data and cross-border data flows are also significant. According to the World Bank, “platform-based business models are increasingly important in low- and middle-income countries.”⁴¹ This includes allowing businesses in developing countries to benefit from the services offered on the global market and to provide data-intensive services in return⁴².

For example, a Bangladeshi firm offers remote assistance to medical doctors in the United States. The doctors wear smart glasses that allow their Bangladesh-based assistants to “witness” patient consultations and create associated medical records. This two-way exchange of data, and the high value-added services they entail, is possible only because both countries—the United States and Bangladesh—allow such sensitive data to move across borders.

The Costs of Limits to Cross-Border Data Flows

In order to understand what is at stake when it comes to data governance, the following provides an overview of the costs of data flow restrictions. Restrictions on data flows affect macroeconomic outcomes and, like tariffs, raise costs and create a deadweight economic loss. The US International Trade Commission in 2014 estimated that the GDP of the United States would be 0.1% to 0.3% higher if data flow restrictions were removed.

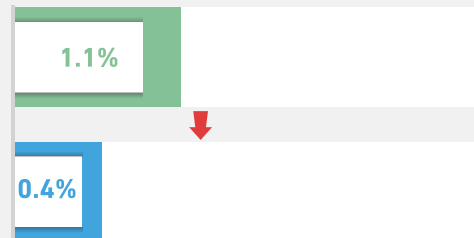
Similarly, for the European Union, barriers to transborder data flows are estimated to reduce GDP by 0.4% to 1.1%, depending on the strength of data localization requirements⁴³. Another study suggests that EU data regulations have reduced real GDP in the European Union by 0.48%⁴⁴.

The negative impact of restrictions on cross-border data flows has been modeled. According to an economic model adopted by Information Technology and Innovation Foundation (ITIF), increases in data restrictiveness negatively impact domestic and international economies by decreasing trade volume and productivity while increasing prices. In the model, 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 chemicals⁴⁵.

These conclusions were bolstered 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



Additional GDP if data flow restrictions are removed



EU - reduced GDP due to barriers to transborder data flows

1.5%

increase in the price of goods and services from industries, such as finance and insurance, petroleum, computers and electrical equipment, and chemicals.

trade and productivity⁴⁶. Another study assessed the GDP impact on 25 countries of removing restrictions on cross-border data flows and found that on average, service imports would increase by 5 percent, benefitting domestic companies and consumers through access to cheaper and better international services⁴⁷. 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 percent⁴⁸.

There is also evidence of the impact of data localization measures on economic growth. In a study of five African countries, data localization was found to particularly increase costs for financial services and undermine productivity growth in manufacturing. One study found that South Africa's GDP would grow by 2.6 percent and investment by 7 percent due to IoT deployment. Still, data localization would undermine these gains, shrinking GDP growth from IoT to 1.1 percent and investment gains to a mere 1.9 percent. Trade, consumption, and employment gains would also shrink⁴⁹.

Another approach to understanding the costs of data localization or data flow restrictions is to look at the potential benefits of reducing policy uncertainty regarding international data transfers and data localization. This was done by the United States International Trade Commission (USITC) when it assessed the economic impact of the United States-Mexico-Canada Agreement (USMCA).



The USMCA chapter on digital trade was one of the main 'new' elements of the old North American Free Trade Agreement (NAFTA). The USITC estimated that the commitments in that chapter to cross-border data flows and avoiding data localization, subject to suitable exceptions, would have a significant positive impact on industries that rely on cross-border data flows. The USITC found that the provisions related to international data transfers are crosscutting in nature and apply broadly to U.S. firms across the economy⁵⁰. These provisions matter for traditional data-intensive internet firms as well as to broader services, manufacturing, and agricultural industries that rely on data and information flows in their business models, supply chains, and international trade.

Limits on cross-border data flows can also increase the cost to businesses of 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 data hosting costs by 30-60%.”⁵¹

Efficiency losses from data localization measures can increase data hosting costs by **30-60%**

Limits on access to data raise costs for firms and hinder firms’ capacity to increase their efficiency. As noted, developing large data sets is an

increasing building block for R&D. Limiting access to and use of data across borders is likely to negatively affect opportunities for global collaboration and innovation.

Data restrictions can also limit access to capital and investment if, say, this means that a lender can’t access financial records. Restrictions on global data flows can also burden the production of goods and the productivity of local companies using digital technologies, particularly in the context of global value chains. A Swedish manufacturing firm recently reported that data localization requirements and restrictions on cross-border data flows, including for outward transfers of data, adversely affected the setup and operation of global production networks⁵².

Insights into the costs of restricting data flows can be obtained from the operation of the European Union General Data Protection Regulation (EU GDPR) which restricts flows of personal data between the EU and third countries. Under GDPR, any business operating outside the EU and processing EU personal data as part of its business operations is under the jurisdiction of GDPR⁵³.

If the third country where the business processes EU personal data has been deemed ‘adequate’ by the European Commission, then personal data can be collected and used. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection⁵⁴. To date, no non EU DCO Member State has received an adequacy finding from the European Commission. In the absence of an adequacy finding, businesses need to turn to Binding Corporate Rules (BCRs) that require the entities of a global conglomerate to treat EU personal data consistently with GDPR.



Another GDPR data transfer mechanism is Standard Contractual Clauses (SCCs) that are included in contracts between an EU entity and a third party to ensure that the treatment of EU personal data is consistent with GDPR. However, both BCRs and SCCs are costly to establish. BCRs, for instance, must be approved by the EU Data Protection Board and are difficult to change.

Moreover, the decision of the Court of Justice of the European Union in *Schrems II* made clear that for BCRs and SCCs to be valid, government access to EU personal data for national security purposes must also be consistent with GDPR rights and obligations⁵⁵. However, in most cases, businesses outside the EU cannot change how their government collects data for national security purposes, in which case BCRs and SCCs may not be available. Compliance with GDPR is enforced by requiring that any business processing EU personal data have a representative in the EU. Fines for non-compliance can be as high as four percent of a corporation's annual worldwide revenue.

The economic impacts of the GDPR have been significant. A July 2018 survey of 539 Mergers and Acquisitions (M&A) 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 GDPR⁵⁶.

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

drop in e-commerce revenue affected by GDPR

13.3%

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 businesses⁵⁷.

1.7-3.4%

less growth in profit for EU firms as compared to their US counterparts

While data flow restrictions have costs associated with them, it is also not the case that no data restrictions are optimal. As noted, data governance regulation is needed to ensure privacy, consumer protection, and national security. The G20 notion of data free flow with trust directly speaks to the need for regulation.

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; 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.

The Different Cross - Border Data Flow Models

The following section assesses a range of laws and regulations that DCO Member States have enacted which affect cross-border data flows. The analysis includes an assessment of each country's goals and their regulations that restrict data flows. The report classifies DCO Member State's data regulations 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"> Consent Adequacy findings Private sector assessment 	<ul style="list-style-type: none"> No a priori mandatory requirements Private sector accountability based on voluntary standards
EXAMPLES	<ul style="list-style-type: none"> Central Bank of Nigeria Data Requirements Oman Cloud First Policy 	<ul style="list-style-type: none"> Guidelines for Nigerian Content Development in ICT Pakistan Prevention of Electronic Crimes Act, 2016 ("PECA 2016") 	<ul style="list-style-type: none"> Saudi Arabia Cloud Computing Regulatory Framework (CCRF) 	<ul style="list-style-type: none"> Bahrain Personal Data Protection Law No. 30 European Union General Data Protection Regulation Saudi Arabia's Personal Data Protection Law ("PDPL") of 2021 amended March 2023 Jordan's Personal Data Protection Law No. 24 of 2023 	<ul style="list-style-type: none"> Oman Personal Data Protection Law

More data closure

Less data closure

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

PART 2: REGULATING FOR A GROWING DIGITAL ECONOMY



Regulations Affecting Data Flows Amongst the DCO Member States

Amongst the DCO Member States, there has been significant cumulative growth in the regulations affecting 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.

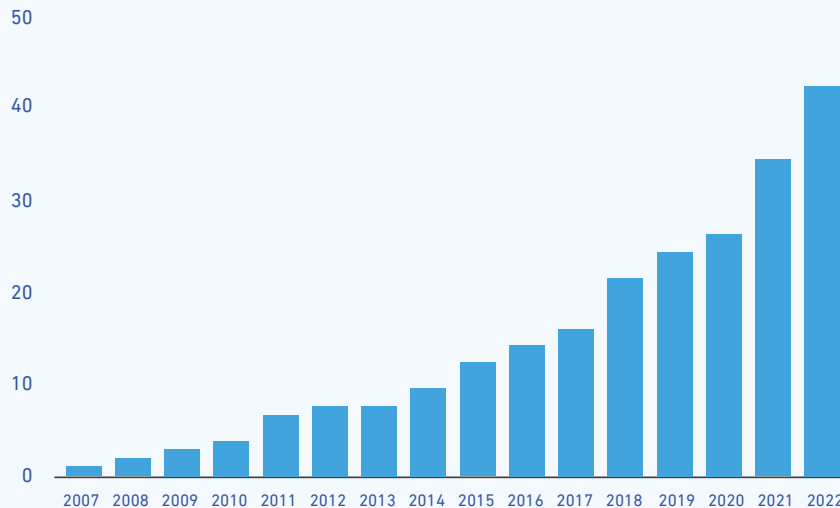


Figure 01. Cumulative Growth in Number of Cross-Border Data Flow Regulations

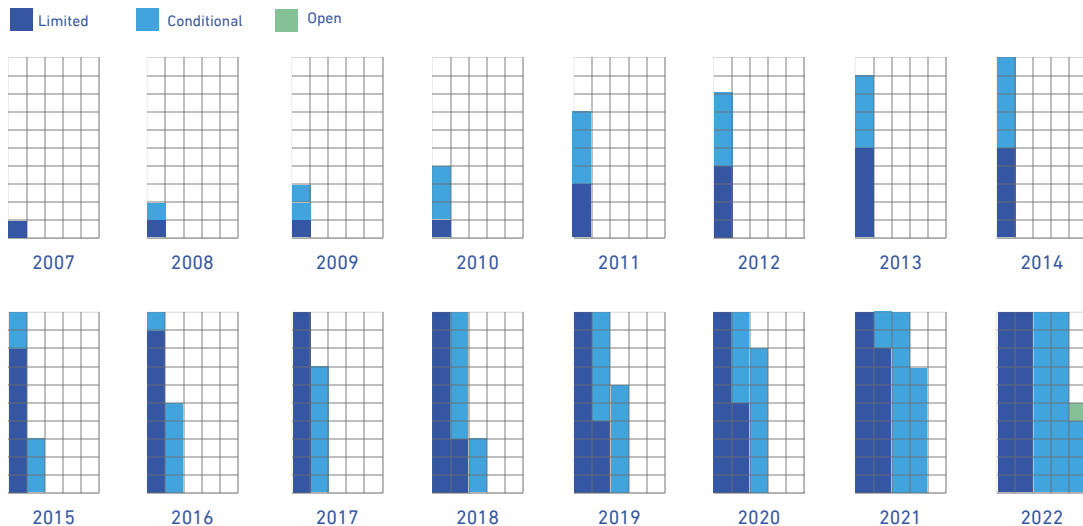


Figure 02. Changes in Data Flow Models Over Time

Figure 02 shows that the growth in data flow regulations has been primarily in the use of '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.

Figure 03 shows distribution of data transfer models across the DCO Member States. The conditional and limited transfers models have been adopted by all the 10 DCO Member States that are included in this report.

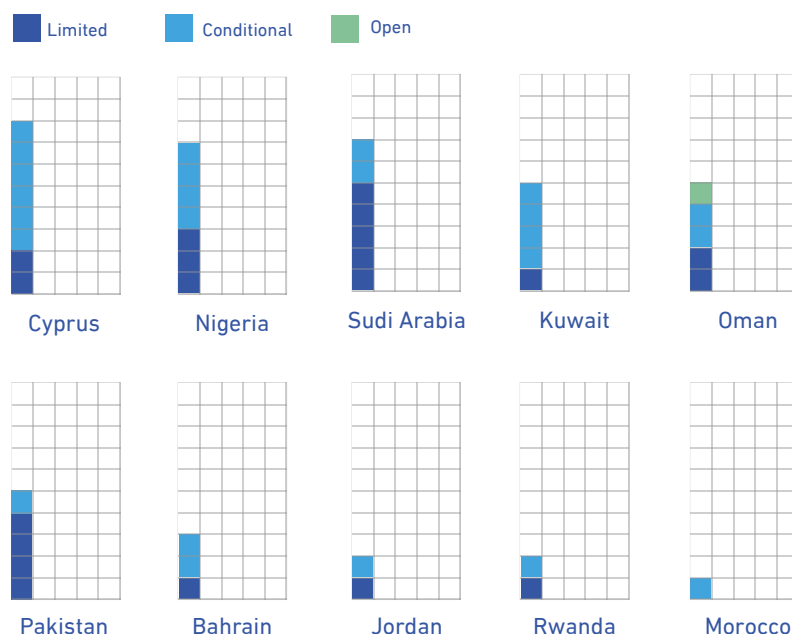


Figure 03. Data Transfer Models by Country

The Key Drivers of Data Flow Restrictions

There is a range of motivations amongst DCO Member States that are driving data governance regulation. As can be seen in Figure 04, 47 percent of the data regulation is about privacy protection, followed by national security, content regulation, financial regulation, and then competition.

Deeper look into the regulatory goals driving the data regulations reveal that privacy regulation has been adopted across all 10 studied DCO Member States. National security is relevant in 70 percent of the countries. Content regulation is a goal in approximately half of DCO Member States.

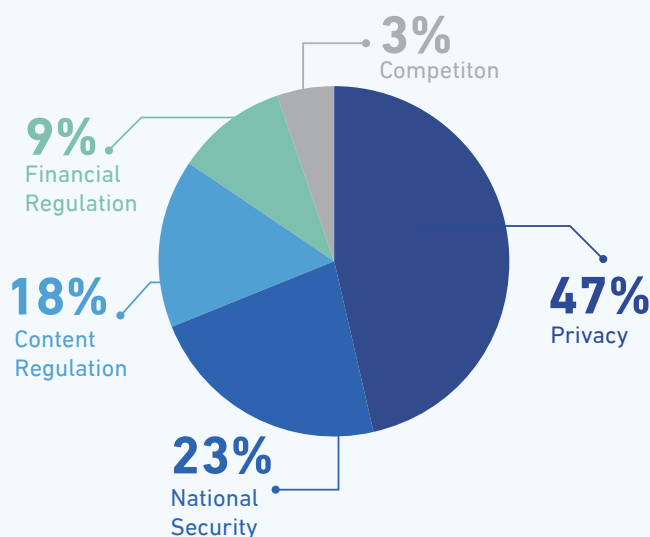


Figure 04. Cumulative Regulatory Objectives of Data Governance Regulations that Affect Cross-Border Data Flows

Figure 05 lists growth over time in data regulations and their objectives. Privacy, content regulation, and national security have been objectives for DCO Member States since 2008. As can be seen, privacy protection has been and remains a key driver of data flow regulation. It was not until 2019, however, that competition also became a policy driver, likely reflecting growing attention to the economic opportunities and challenges in building a digital economy.

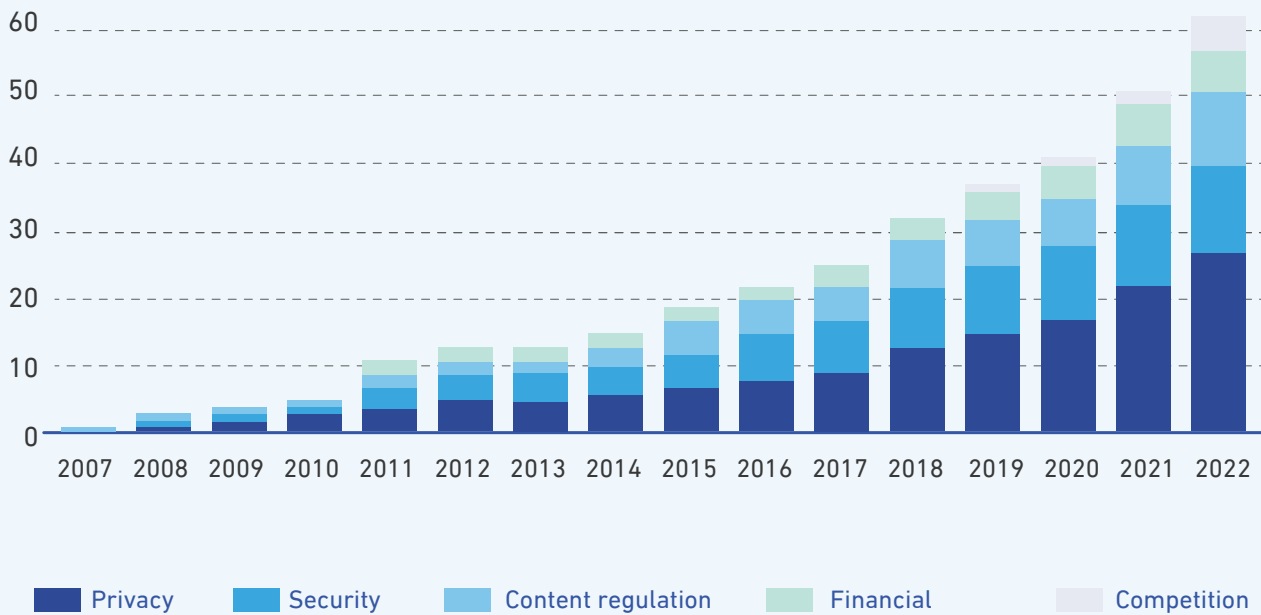


Figure 05. Number of Data Regulations by Regulatory Objective Over Time

PART 3: ENABLING CROSS-BORDER DATA FLOWS AND REGULATION



Getting to the G20 Goal of Data-Free Flows with Trust

As noted, a key enabler of the digital economy will be appropriate regulation coupled with cross-border data flows. There is already high-level recognition amongst many governments, including some 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

The G7 has also provided guidance on how to support data flows and digital trade. In 2021 the G7 released G7 Digital Trade Principles, which states that "data should be able to flow freely across borders with trust" and elaborates on how to balance opportunities from data flows with the need for domestic regulation that might restrict cross-border data flows⁵⁸. For instance, there is recognition of the need to "address unjustified obstacles to cross-border data flows while continuing to address privacy, data protection, the protection of intellectual property rights, and security."⁵⁹

Developing interoperability mechanisms aimed at specific regulations or types of data will require a framework amongst the DCO Member States to enable data free flow with trust. What constitutes data free flow with trust and how it can be operationalized remains under development, including in the G7 this year. The current state of play presents the DCO Member States with an opportunity to lead in developing interoperability mechanisms and informing what is meant by data free flow with trust globally. Several project-orientated steps are practical and could support cross-border data flows:

1. Assess and support the development of privacy-enhancing technologies that can enable compliance with domestic privacy laws and cross-border data flows. The US and the UK have developed a prize challenge to incentivize the development of privacy-enhancing technologies, and a similar approach could be taken amongst the DCO Member States. Developing privacy-enhancing technologies also present opportunities more broadly to use personal data, whether for AI or healthcare and to collaborate amongst governments on shared challenges such as financial crimes and pandemic responses⁶⁰. Regulatory technology is another area where the application of technology can support regulatory efficiency across borders. In all these areas, it would require bringing together groups of industry and government officials and civil society around specific project opportunities to assess barriers, opportunities, and ways forward.
2. Increased transparency of each DCO Member States' laws and regulations as they affect cross-border data flows can build trust. One project would be for the DCO Secretariat to build a database of regulation that affects data flows. This would allow all DCO Member States to understand the data governance regulations. The next step would be to develop a process for ongoing notification of new data governance regulations as well as changes to these laws and regulations.



Interoperability and Cross-Border Data Flows

Interoperability mechanisms enable cross-border data flows while respecting differences in data governance regulation. In this respect, interoperability mechanisms enable data free flow with trust. The importance of developing interoperability mechanisms to enable cross-border data flows is reflected in Leader's statements at the G20 and the G7 and in various bilateral and regional digital economy agreements. 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."⁶¹ At the Rome G20 in 2020, Leaders identified the need to "work towards identifying commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability."⁶² The G7 recognized the need to "cooperate to explore commonalities in our regulatory approaches and promote interoperability between G7 members."⁶³ Interoperability is also a subject of bilateral discussion and negotiation, as well as discussion in international economic forums such as APEC, ASEAN, and the OECD.

"we will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development"

2019 Osaka G20 Leaders Declaration

Interoperability is not premised on the harmonization of data governance regulation. Instead, interoperability focuses on ends or goals and seeks to avoid data flow restrictions based merely on different approaches or means. Interoperability is helped by some convergence towards similar or closely related goals, particularly when it comes to government-permissioned data flows. In other cases where industry or individuals are able to decide where data flows and assume responsibility for that data's protection, there is more scope for data flows even where the countries where the data is flowing might protect data differently from home or exporting country.



This potential flexibility of interoperability mechanisms reflects the reality that a global alignment on data governance laws and regulations, such as privacy, financial regulation, and national security, is unlikely. Moreover, the pursuit of interoperability underscores that lack of regulatory alignment should not be a barrier to cross-border data flows.

Interoperability in Trade Agreements and Digital Trade Agreements

The importance of cross-border data flows for digital trade and enabling interoperability is also an increasingly prominent feature in free trade agreements that include digital trade chapters and digital economy agreements (DEAs). Figure 06 outlines key digital trade commitments in major trade agreements, including those relevant to data flow and encouraging interoperability.

<div> <div></div> Required <div></div> Best endeavors <div></div> None </div>		RCEP (2021)	CPTPP (2018)	SINGAPORE-AUSTRALIA DEA (2020)	DEPA (2020)	USMCA (2019)	EU-JAPAN EPA (2019)
Trade Facilitation	Paperless trading						
	E-invoicing						
	Electronic authentication and signatures						
	Digital ID						
	No customs duties on transmissions	1					
	Non-discrimination between digital products						
	Access to and use of the internet, services, and applications						
	Digital payments						
Building Trust	Protection of online personal information						
	Cybersecurity						
	Consumer protection						
	International standards			2	3		
	Address unsolicited commercial messages						
Data Flows	Cross-border transfers of information	4	5	5	5	5	
	Avoid data localization	4	5	5	5	5	
	Not require source code		5	5		5	5
Emerging Tech	Digital technologies, i.e., AI, Blockchain						

Figure 06. Key Digital Trade Commitments in Major Trade Agreements

KEY

- 1 Consistent w/ WTO moratorium; 2 Mix of binding & best endeavors; 3 E-invoicing; 4 With expanded exception; 5 With GATS-style exceptions
- RCEP (2020) Regional Comprehensive Economic Partnership. Participants: Australia, New Zealand, Brunei, Cambodia, China, Japan, Laos, Singapore, Thailand and Vietnam
- CPTPP (2018) Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Participants: Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam
- Singapore-Australia DEA (2020) Singapore-Australia Digital Economy Agreement
- DEPA (2020) Digital Economy Partnership Agreement. Participants: Chile, New Zealand and Singapore
- USMCA (2019) United States–Mexico–Canada Agreement
- EU-Japan EPA (2019) EU-Japan Economic Partnership Agreement



As can be seen, commitments to cross-border data flows subject to suitable exceptions are now common across many trade agreements, including the Regional Comprehensive Economic Partnership (RCEP) amongst China, ASEAN Member States as well as Australia, Japan, New Zealand, and South Korea. Notably, the EU has yet to make this commitment in trade agreements.

It is also increasingly common to find commitments to avoid data localization as a requirement for doing business, again subject to suitable exceptions based on the WTO General Agreement on Trade in Services (GATS)⁶⁴. This includes commitments in regional trade agreements such as the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), United States–Mexico–Canada Agreement (USMCA), as well as digital economy agreements such as the Digital Economy Partnership Agreement (DEPA) and bilaterally between Australia and Singapore.

The role of the exceptions provisions in trade agreements is to provide regulatory space to restrict data flows to achieve legitimate public policy goals but also to require that

restrictions are “necessary.” What is meant by “necessary” has been interpreted by the World Trade Organization (WTO) Appellate Body as requiring that it is no less trade restrictive than necessary⁶⁵.

This means that in these trade agreements, governments have agreed that restricting data flows to achieve a legitimate public policy objective, such as privacy, must be the least restrictive of data flows.

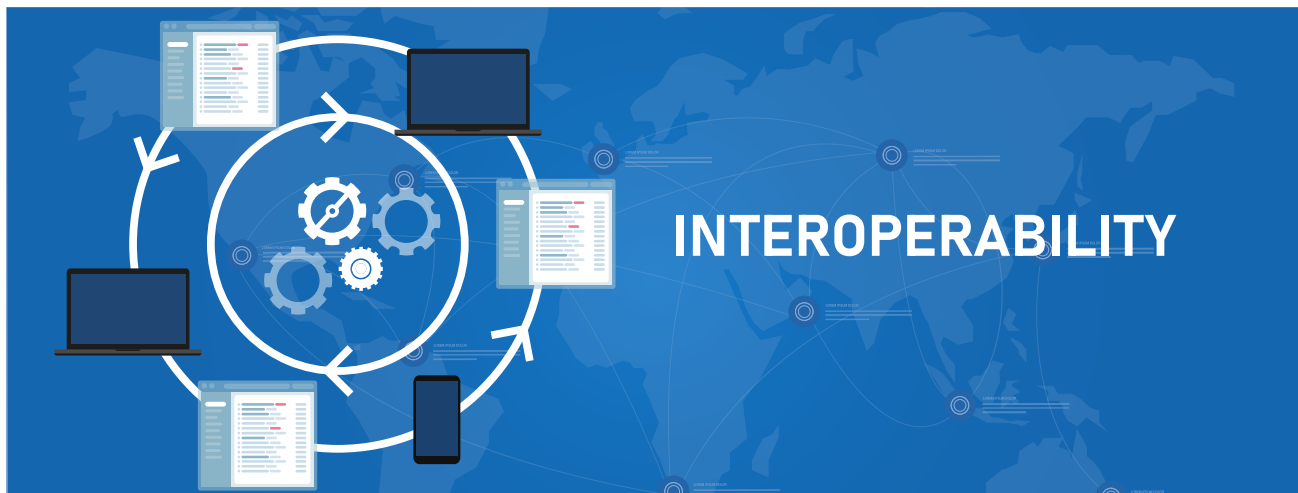
Worth noting here is that while RCEP includes commitments to data flows and no data localization commitments, the exceptions provision is considerably broader than these other trade agreements where the exceptions are based on the WTO GATS exception provision. Instead, in RCEP the determination as to whether a measure is “necessary” is up to the party enacting the measure to decide. In contrast, under the GATS Article XIV style exceptions, it is an objective assessment of fact as to whether the measure is necessary i.e., least restrictive of data flows. The effect of this difference is to give much greater scope to parties to RCEP to restrict data flow compared with under CPTPP or USMCA.

In addition to these commitments, digital trade chapters and digital economy agreements also include commitments supporting interoperability mechanisms' development. For example, CPTPP states that the parties will “encourage the development of mechanisms to promote compatibility between these different regimes.

These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement or broader international frameworks.”⁶⁶ USMCA states that each party should encourage the

development of mechanisms to promote compatibility between these different regimes. The parties to USMCA “recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information” — another way of saying that this is an interoperability mechanism.

As discussed in more detail below, digital trade chapters and digital economy agreements are also supporting interoperability amongst digital payment systems and digital IDs.



Developing Interoperability Mechanisms

As outlined, key drivers of data flow restrictions amongst the DCO Member States are privacy, content regulation, financial regulation, and national security. Interoperability can be developed regionally or bilaterally. Analysis of the DCO Member State regulation 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 two main types of interoperability mechanisms:

Unilateral recognition of another country's regulation as equivalent in effect, allowing data to flow freely to that country. For example, Country A would recognize Country B's privacy regulation as equivalent, allowing personal data from Country A to flow to Country B. Nothing more is required from Country B. This option, while available, is often not pursued in practice because there are real differences among the country's regulations that prevent unilateral recognition. This report does not address this type of interoperability any further.

Mutual recognition of equivalence: here, both countries agree to recognize each other's regimes as equivalent. Developing such an interoperability mechanism has three elements, and each element is worth pursuing on its own. The first element is agreeing on common principles — whether with respect to privacy, financial payments, or consumer protection. The second element is agreement on a data classification scheme that will guide regulation and entities holding data. The third is an agreement to establish cross-border institutional mechanisms that will allow each country to treat the other's domestic data governance regulation as equivalent such that data can flow freely between them.

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

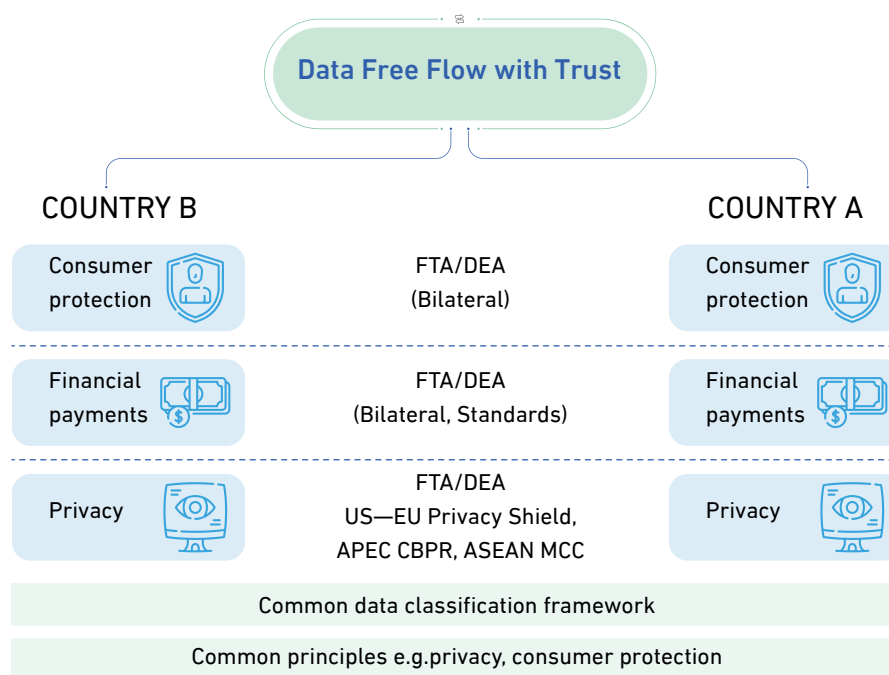


Figure 07. The Building Blocks of Interoperability

Agreeing on common principles and a data classification scheme provides a foundation for targeted bilateral and regional interoperability mechanisms that will enable data-free flows with trust.

Agreeing on common principles has two primary purposes. The first is to limit the diversity of domestic regulation where countries can agree to base their domestic regulation on these principles. This, for instance, has been the role of the OECD Privacy Principles, the APEC Privacy Framework, and the ASEAN Privacy Principles. The second related role of agreeing on principles is to provide a baseline against which equivalence can be assessed and on which interoperability schemes are built. This is outlined in more detail below; suffice to note here that commonly agreed privacy principles can give the data exporting country confidence in the level of privacy protection in the data importing country.

Though there is no global agreement on data classification, as outlined above, the DCO Member States are increasingly classifying data, and early efforts are underway to develop a more common approach across countries. A data classification scheme would serve two primary purposes. It would allow for a more targeted discussion on which data needs to be limited and which can flow freely. Second, it would guide entities that collect data on data segmentation strategies that can also help minimize cross-border data flow restrictions.

The institutional mechanism that will be needed will vary depending on the data covered by the interoperability mechanism and the scheme itself. As will be articulated more fully with respect to interoperability for personal data, institutional mechanisms can include third-party oversight of compliance, third-party audits, and additional rights or commitments to raise the level of regulatory protection to achieve equivalence.

Agree on a Data Classification Scheme



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 drawn in early data classification efforts has 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 Union⁶⁷. The World Bank also advocates a distinction

between personal and non-personal data, with different regulatory approaches for each one⁶⁸. 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. The following image shows these data categories and their areas of overlap.

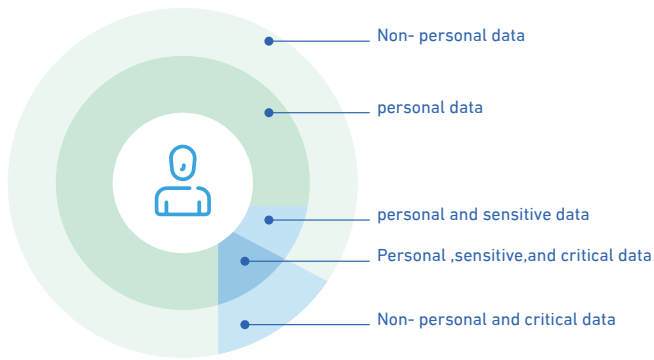


Figure 08. Data Classification

Many of these data classifications are being used by the DCO Member States. For example, specific initial attempts at data classification are being made under the Kuwait Cloud Computing Regulatory Framework, Oman's Cloud Computing Policy, and Saudi Arabia's Personal Data Protection Law ("PDPL") of 2021, amended March 2023⁶⁹ and Saudi Cloud Computing Regulatory Framework⁷⁰. Pakistan's Draft Personal Data Protection Bill*, Rwanda's Law on the Protection of Personal Data and Privacy 2021, Bahrain's Personal Data Protection Law No. 30, and Nigeria's Draft Data Protection Bill 2020* distinguish between personal data and critical data. The European Commission defines personal data as information relating to an "identified or identifiable living individual." Examples include an individual's name, home address, or location data, such as from a mobile phone⁷¹. Personal data considered sensitive has a narrower scope, referring to "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs," as well as an individual's trade-union membership, genetic data, health-related data, and data concerning a person's sex life or sexual orientation⁷².

According to the EU's Regulation on a Framework for the Free Flow of Non-Personal Data Regulation on a Framework for the Free Flow of Non-Personal Data, examples of non-personal data include "aggregate and anonymized datasets used for big data analytics" or "data on maintenance needs for industrial machines."⁷³ According to Pakistan's Draft Personal Data Protection Bill*, critical personal data includes "data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations." Sensitive personal data is defined as "data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, computerized national identity card, passports, biometric data, and physical, behavioral, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, political affiliation, identifiable physical location, traveling details, pictorial or graphical still and motion forms, IP address and an online identifier." Personal data is "any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in possession of a data controller and/or data processor, including any sensitive personal data."⁷⁴

Bahrain's Personal Data Protection Law No. 30 defines data or personal data as "any information in any form concerning an identified individual, or an individual who can, directly or indirectly, be identified by reference, in particular, to his or her personal identification number, or by reference to one

* Disclaimer: Please note that the reference has been made to a draft law which is subject to changes upon final approval. The information provided is based on the current version of the draft law as of the date of this disclaimer. Any modifications or amendments made to the law during the approval process may affect the accuracy or applicability of the information provided. Therefore, it is recommended to consult the final version of the law once it is approved for any official or legal purposes.

or more factors specific to his or her physical, physiological, intellectual, cultural, economic, or social identity. In determining whether an individual is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.” The law further defines sensitive personal data as “any personal information revealing — directly or indirectly — about an individual’s race, ethnical origin, political or philosophical opinions, religious beliefs, affiliation to a union, personal criminal record, or any information in relation to his health or sexual status.”⁷⁵



Rwanda’s law governing data protection defines personal data as “any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of that natural person.”⁷⁶ Sensitive data is defined as “information revealing a person’s race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life, or family details.”⁷⁷

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 data will increase as data is seen as increasingly sensitive or critical, with more free flow of data for non-personal data that does not pose any national security concerns.

Going forward, a common taxonomy of data classifications could be developed for the DCO Member States. This would provide an important foundation for a data classification scheme. A common approach to data classification would help identify opportunities for interoperability. For instance, trust that countries are categorizing what is sensitive personal data according to common criteria or standards would shift the conversation to how to protect that data while also allowing data to flow.

PART 4: DEVELOPING INTEROPERABILITY MECHANISMS



Privacy Regulation and Cross-Border Data Flows

Privacy regulation has emerged as the most important source of data flow restrictions. There is also a range of privacy regulations and different impacts on cross-border data flows. Figure 09 shows that all ten DCO Member States studied in the report have privacy regulations.

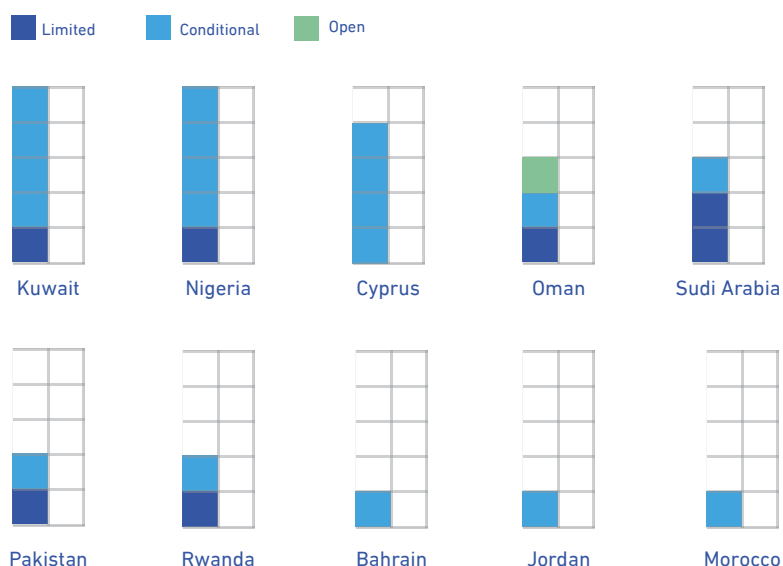


Figure 09. Privacy Regulation by Country and Data Transfer Model

The majority of DCO Member State's privacy regulations adopt a conditional transfers model. In most cases, this means that there is some type of adequacy requirement before personal data can flow to the country receiving the personal data. Adequacy requires that the destination country has in place a certain level of guaranteed protection, the outstanding question being what constitutes adequacy. Notably, many of the regulations in this group either explicitly or implicitly reference other international regulations or considerations. For example, Bahrain's Personal Data Protection Law No. 30 "accounts for data that would fall under protected characteristics of individuals under EU human rights law." Morocco's National Commission for the Protection of Personal Data Protection (CNDP)

uses the country's Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data as a foundation on which updates and revisions can be added to "comply with international data protection requirements" and "further align it with global standards." The implementation framework for Nigeria's 2019 Nigerian Data Protection Regulation states that, "where the NDPR and this Framework do not provide for a data protection principle or process, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 and European Union General Data Protection Regulation (EU GDPR) and its judicial interpretations shall be of persuasive effect in Nigeria".

Most countries with personal data protection laws and regulations in this dataset follow the adequacy approach. However, this approach to personal data is not yet a monolith. For example, Oman's Personal Data Protection Law is an open transfer model as it relies on a relatively straightforward consent mechanism by which individuals must accede to data processing requests that are "clear, explicit, and understandable." Saudi Arabia's Amended Personal Data Protection Law⁷⁸ is a conditional transfer model, and the recent amendments bring Saudi approach to privacy closer to the GDPR.

Existing Privacy Interoperability Mechanisms



Several interoperability mechanisms are being developed that enable cross-border transfers of personal data, which can guide work by the 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 are the ASEAN model contractual clauses (MCC) and the US-EU Privacy Shield 2.0. Each interoperability mechanism demonstrates different potential approaches and scope to accommodate divergent domestic privacy

rules, which is important amongst these DCO Member States given the divergence in approaches to privacy. The following outlines each of the main interoperability mechanisms for personal data.

The EU General Data Privacy Regulation:

Under the GDPR, data can be transferred outside the EU only if specific conditions are fulfilled. The main one is where the European Commission has found that the third country receiving personal data provides adequate protection.⁷⁹ In the absence of an adequacy decision, the GDPR allows data to be transferred outside the EU pursuant to various safeguards or derogations⁸⁰.

According to the Court of Justice of the European Union (CJEU), a finding of adequacy requires other countries to have in place a privacy regime that is 'essentially equivalent' to that of the EU ⁸¹.

In the absence of an adequacy finding, the GDPR provides several mechanisms for transferring personal data to another jurisdiction. ⁸² Each mechanism needs approval by either the European Commission or a Member State privacy authority. The main ones are binding corporate rules (BCRs), standard contractual clauses (SCCs), an approved code of conduct, or an approved certification mechanism. The latter two options remain underdeveloped in the EU, so the focus here is on BCRs and SCCs. As discussed, BCRs allow multinational companies to move EU personal data globally within the conglomerate. BCRs must be legally applied and confer enforceable rights on data subjects. ⁸³ In addition, to establish a BCR, GDPR requires a controller or processor who can be held liable for a breach to be established in a Member State. ⁸⁴ SCCs allow for transfers of personal data outside the EU to third parties. Such contracts require the same levels of protection, oversight, and access for individuals as would be the case with an adequacy decision.

Data transfers to third countries are also allowed based on so-called derogations from GDPR. The main ones are explicit consent by the data subject, transfers necessary for the performance of a contract between the data subject and the controller, or transfers necessary for the purposes of a legitimate interest pursued by the controller, which cannot be qualified as frequent or massive ⁸⁵. These derogations are not suitable for large-scale regular transfers of data and are, therefore, not a foundation for building an interoperability mechanism.

Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System: Building on the APEC Privacy Principles — last updated in 2015 and which itself is based on the OECD Privacy Principles — APEC Cross-Border Privacy Rules (CBPRs) facilitate the transfer of personal information among APEC Members. The CBPR requires businesses to develop privacy policies based on the APEC privacy principles, which meet the CBPR program requirements. APEC Accountability Agents, independent third parties certified domestically, are tasked with assessing the consistency of businesses' privacy policy and practice with the APEC CBPR requirements. Businesses that meet the CBPR requirements



and are subject to the laws of an APEC CBPR participating economy can be certified as compliant. Currently, the USA, Mexico, Japan, Canada, Singapore, Korea, Australia, and Chinese Taipei are participating in APEC CBPRs. APEC Accountability Agents and Privacy Enforcement Authorities enforce compliance by businesses with APEC CBPR requirements.⁸⁶ The ability for countries outside APEC to participate in APEC CBPRs is being pursued following the launch of the Global CBPR Forum⁸⁷.

US-EU Privacy Shield 2.0: Under the Privacy Shield 2.0, US companies, through an industry body or individually, self-certify to the US Department of Commerce that they will protect the personal data of EU citizens consistent with the Privacy Framework, which includes the Privacy Shield Principles⁸⁸. The process to develop Privacy Shield 2.0, also known as the Trans-Atlantic Data Privacy Framework, became a necessity in 2020, when — for the second time — the Court of Justice of the European Union (CJEU) struck down European Commission’s finding that the previous Privacy Shield was “adequate.”⁸⁹ According to the CJEU, US Executive Order 12333 and FAA 702 do not meet the necessity

and proportionality standards in Article 52 of the EU Charter on Human Rights or the requirement for actionable judicial redress for EU citizens in the charter⁹⁰.

After nearly two years of negotiations, the United States and the European Commission announced in March 2022 that they had agreed in principle on a new Trans-Atlantic Data Privacy Framework that addresses the concerns raised by the CJEU in *Schrems II*.

In October 2022, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, implementing the EU-U.S. Data Privacy Framework (EU-U.S. DPF) agreed upon in March. Among other steps, the Executive Order adds further safeguards to U.S.

March 2022 US -EU agreed on Trans-Atlantic Data Privacy Framework

signals intelligence activities, mandates requirements for the handling of personal information gathered through signals intelligence, and creates a new mechanism for EU individuals to seek redress if they believe that their personal information is unlawfully collected or handled by the United States^{91 92}.

The European Commission describes this new redress mechanism, which would replace the current Privacy Shield Ombudsperson, as a “two-layer” redress mechanism with “independent and binding authority.” The first layer would allow individuals in the EU to file a complaint with a Civil Liberties Protection Officer representing the U.S. Intelligence Community. The

“two-layer” redress mechanism with “independent and binding authority.”

second layer would facilitate appeals to the decisions of the Civil Liberties Protection Officer through a newly formed Data Protection Review Court, which would be composed of members from outside the U.S. government.

The Court will be empowered — where the Ombudsperson was not — to investigate the complaints of EU individuals, including through the ability to obtain relevant information from the intelligence community and the power to hand down binding remedial decisions. Moreover, in reviewing each case, the Court will appoint a special advocate to ensure that the complainant’s interests are equitably represented⁹³.

ASEAN Model Contractual Clauses (MCC):

The ASEAN MCCs are contractual terms and conditions that may be included in legal agreements between parties transferring personal data to each other across borders⁹⁴. MCCs help parties ensure that the transfer of personal data is done in a manner that complies with ASEAN Member States’ (AMS) legal and regulatory requirements and protects personal data consistently with the principles of the ASEAN Framework on Personal Data Protection (2016). The



ASEAN Privacy Framework on Personal Data Protection (The Framework) is a non-binding statement of principles to guide the protection of personal data and the data subjects rights. The Framework aims to promote electronic commerce throughout the ASEAN region and is consistent with the core values of the OECD’s Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines).

The MCCs are templates that set out the responsibilities, personal data protection measures, and related obligations of the parties. The MCC was developed to enable personal data flow amongst countries with significantly different levels of development. Private sector parties in ASEAN Member States may voluntarily adopt the MCCs to support the transfer of personal data to parties in other ASEAN Member States. While the MCCs are primarily designed for the intra-ASEAN flow of personal data, parties may adapt these clauses with appropriate modifications at their discretion for transfers to outside ASEAN, particularly those with legal regimes based upon the principles of the APEC Privacy Framework or OECD Privacy Guidelines⁹⁵.

The following table outlines these main privacy interoperability mechanisms as well as their main points of similarity and difference.

TABLE 02: Main Privacy Interoperability Mechanisms Data Flows

	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"> • An adequacy decision where the privacy regime is essentially equivalent. • BCRs • SCCs 	<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"> • EU Commission assesses and grants adequacy. • EU Data Protection Authorities approve BCRs and SCCs. 	<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"> • None for adequacy • Responsible for ensuring compliance with SCC or BCR. 	<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>

Developing Interoperability for Cross-Border Flow of Personal Data

These interoperability mechanisms for personal data point to a range of possibilities for developing interoperability mechanisms amongst the DCO Member States. The interoperability mechanisms could be bilateral, regional, or amongst all countries. The inclusion of Cyprus as a member of the EU will mean that any mechanism that includes Cyprus will have to be GDPR consistent, and in particular, an adequacy decision can only be made by the European Commission. BCRs and SCCs will need to be certified by 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.



1. Agree privacy principles

The first step should be to agree on common privacy principles. There is already common ground among many DCO Member States whose privacy laws are built on OECD Privacy Principles and have been influenced by GDPR. A common baseline of privacy principles that all countries agreed on would be a key enabler of various interoperability mechanisms that will allow data flows. If not amongst all DCO Member States, then an agreement should be reached with a subset of Member States.

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 regulatory efforts at interoperability. It would also provide guidance to entities collecting personal data on how to best categorize personal data.

3. Agree on conditions under which data can flow

Building on common privacy principles and agreement on data classification, various approaches could be adopted to develop interoperability tailored to each country's approach to privacy:

a. Where adequacy is required in the country receiving the personal data, each DCO Member State government could assess whether any of the other countries here are adequate. Ideally, this could also be agreed to be done on an expedited basis with the aim of prioritizing adequacy amongst DCO Member States. This will also require defining adequacy, and here there are broadly 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.

As noted, the approach of Cyprus to what constitutes adequacy will be determined by the European Commission under GDPR and would require essentially equivalent levels and forms of privacy protection in other countries. Given this, DCO Member States should assess the likelihood of successfully getting an adequate finding from the European Commission to enable flows of personal data between Cyprus and other DCO Members and assess the validity of BCRs and SCCs. Separately, the DCO Member States could also develop an everyone but EU (currently Cyprus) strategy for enabling flows of personal data that is more flexible than GDPR. This could start by defining adequacy as requiring that the data destination country provides comparable or similar levels of privacy protection.

b. Develop specific interoperability mechanisms similar to the US-EU Privacy Shield. For instance, businesses in the DCO Member

States could self-certify into a government-led scheme supported by third-party oversight of compliance. Participation in the scheme would guarantee that privacy protection was consistent with any agreed-upon privacy principles. Another option in the absence of agreement on privacy principles would be that the entities participating would treat the personal data consistent with the privacy protection in the data exporting country. This would be a form of adequacy but would only be available for entities that can demonstrate a capacity to meet the other (presumably) higher privacy standards.

c. A third approach would be to develop a certification scheme along the lines of APEC CBPR where businesses receive a recognized certification where they can demonstrate privacy policies consistent with commonly agreed privacy principles. Entities in countries requiring adequacy before exporting personal data could agree to allow cross-border flows of personal data to certified businesses in other DCO Member States.

d. DCO Member States could also agree on standard contractual clauses that, when included in contracts with third parties, achieve an adequate level of privacy protection. This approach would rely more on business accountability. Still, it could include an agreement by domestic authorities to enforce compliance by such businesses with their privacy policies and/or an agreement to establish a process for auditing compliance by businesses with their privacy policies.

Supporting Cross Border Payments

Cross-border payments rely on the exchange of data to work. Enabling cross-border payments at the retail and wholesale levels can reduce the costs of international e-commerce, expand opportunities for businesses to participate in digital trade, and improve flows of remittances which are particularly important for many of these countries. For

instance, The United Nations Sustainable Development Goal 10 aims to reduce to less than 3 percent the transaction costs of migrant remittances

The UN SDG Goal 10 aims to:

- Reduce to less than **3%** the transaction costs of migrant remittances
- Eliminate remittance corridors with costs higher than **5%**

and eliminate remittance corridors with costs higher than 5 percent. As outlined above, financial regulation is an important reason for data flow restrictions. 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.

Interlinking payment systems will require data flows of financial information. This would allow Payment System Providers (PSPs) in Country A to send payments to PSPs in Country B without the need for Country A's PSP to open accounts in Country B or become a participant in Country B's payment system. PSPs currently often use the services of local agents or correspondent banks to facilitate the transaction. Current arrangements lead to long chains, delays, and greater costs. As a



result, cross-border payments lag significantly behind domestic payments in meeting user expectations for services that are cheap, fast, accessible, and transparent. Wholesale payments are typically processed through a chain of banks. In contrast, cross-border retail payments often rely on closed-loop systems — a single platform connecting payee and payer — eliminating the need for a connection between institutions or infrastructure in the two jurisdictions. A range of regulations and standards related to cross-border payments create costs and delays.

New technologies and increasing standardization and application programming interfaces (APIs) can enable even greater interoperability, with the potential to interlink arrangements to improve the efficiency and transparency of cross-border payments. APIs are messengers that run with an instruction from the requestor to the information provider and back again with the answer. APIs enable software applications e.g., mobile phone apps, to request specific data from another software application and for data transfers from the data providing the application back to the requestor. APIs can provide a network-neutral means for the exchange of financial

data. With appropriate security features, APIs can enable the exchange of financial data across virtually any telecommunication financial messaging network, public or private, including the internet. Payment platforms are increasingly using ISO 20022 messaging standards, but differences in the implementation of ISO 20022 are slowing progress.

In 2020 the G20 endorsed a roadmap to enhance cross-border payments. The G20 established five core building blocks (work streams) running in parallel:

- 01** Committing to a joint public and private-sector vision to drive change.
- 02** Coordinating regulatory, supervisory, and oversight frameworks to identify gaps or areas for further alignment, where appropriate.
- 03** Improving existing payment infrastructures and arrangements, with a focus on widening availability, strengthening links between payment systems, and reducing settlement risks.
- 04** Increasing data quality and straight-through processing by enhancing data and market practices.
- 05** Exploring the potential role of new payment infrastructures and arrangements.

These types of steps would support and encourage the linking of payment systems.

Steps to Facilitate Cross-Border Payments Systems

DCO Member States could take a range of steps to facilitate cross-border payments. This includes Foreign Digital Investment (FDI) frameworks and alignment on regulatory guidance and frameworks applicable to cross-border payments, including rules on consumer protection, privacy, and regulation of financial sectors to achieve trust and security that is predictable and appropriate to the risks posed by the provision of electronic payment services.

For instance, this can include aiming to align International Organization for Standardization (ISO) 20022 Universal Financial Message Scheme messaging standards and avoiding regulation that prevents trading in currencies across borders.

Countries could consider bilateral or regional agreements to cooperate on these issues. For instance, the Digital Economy Partnership

Agreement and the Australia-Singapore Digital Economy Agreement include commitments to support cross-border electronic payments.

There are a range of steps DCO Member States could take to promote interoperability and the interlinking of their electronic payment infrastructures:

- a.** Modernize the regulation on consumer protection, privacy, 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 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 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.

These types of steps would support and encourage the linking of payment systems.

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 regional agreements on digital IDs. As discussed, 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^{96 97}. Nigeria's National Identity Management Commission (NIMC) is playing a central role in developing Digital IDs by registering all citizens with Unique National Identification Numbers⁹⁸.

Some countries are already developing digital ID rules in digital trade agreements. This could be done as part of a trade agreement or as a stand-alone bilateral or regional agreement on digital ID. For example, in the Digital Economy Partnership Agreement, the parties “endeavor to promote the interoperability between their respective regimes for digital identities.”



Nigeria has reached nearly

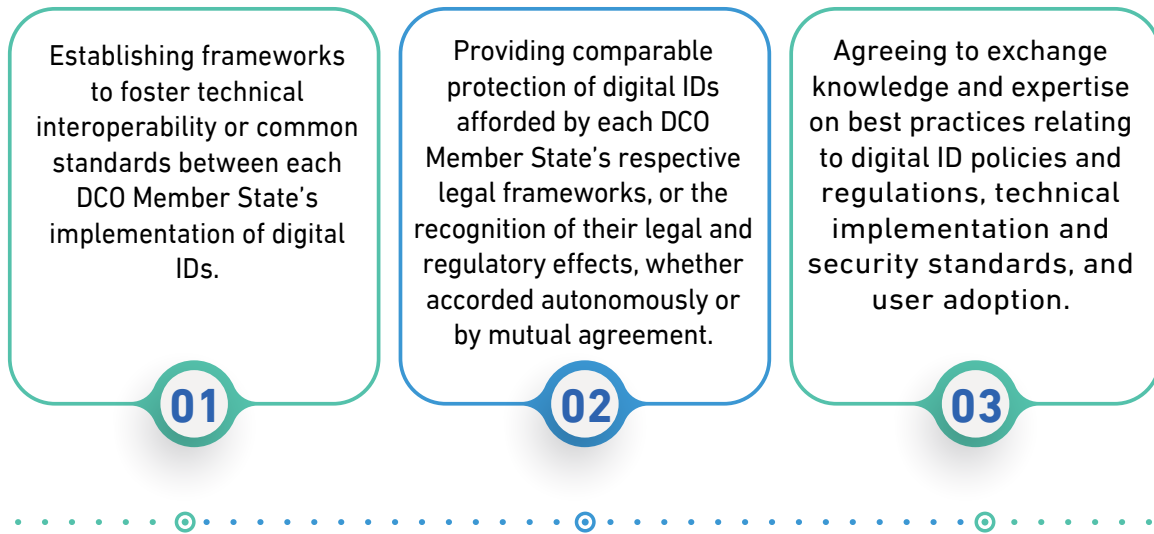
90 million

enrollees in its World Bank-funded Nigeria Digital Identification for Development (ID4D) project, with a goal of enrolling 140 million people by 2024

“endeavor to promote the interoperability between their respective regimes for digital identities”

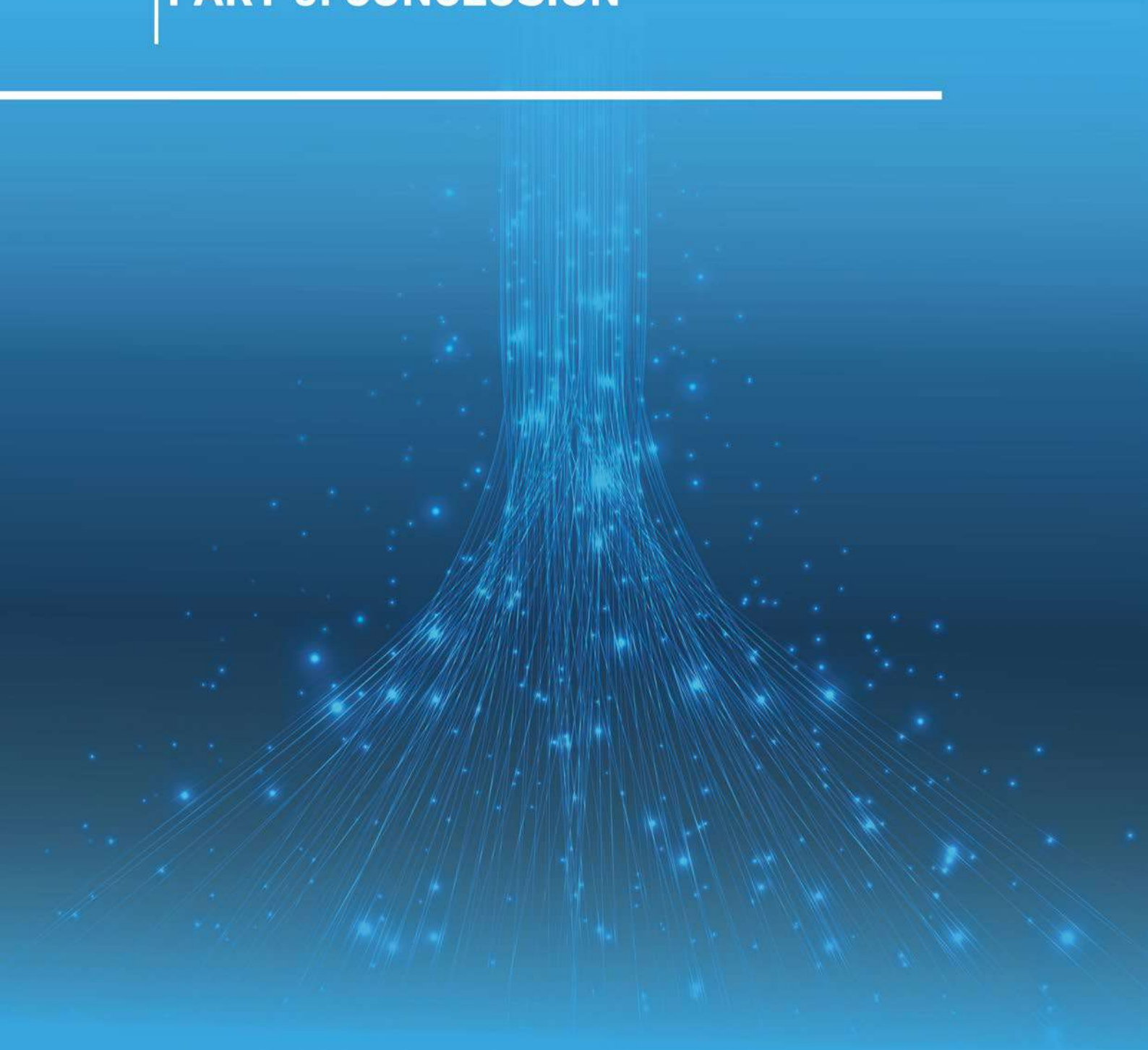
Digital Economy Partnership Agreement

Steps that DCO Member States could take drawing on progress in DEAs include:



These types of government-to-government agreements provide the legal and regulatory frameworks that can enable cross-border recognition of digital IDs.

PART 5: CONCLUSION



Most DCO Member States have implemented comprehensive data governance regulations in areas such as privacy, finance, content regulation, and national security. These data governance regulations also limit cross-border data flows, with costs for economic growth and trade, as well as for business operations and innovation. All DCO Member States have prioritized expanding their digital economies, which to be successful, will require enabling access to and use of data. While data regulation has costs, it is also needed to create trust amongst government, business, and consumers that access to the data is being used consistent with national standards. **The challenge and the opportunity for the DCO Member States are to develop interoperability mechanisms that enable cross-border data flows while also maintaining the regulatory autonomy to achieve legitimate public policy goals.** Interoperability mechanisms are an opportunity to do just that - enable cross-border data flows and preserve digital regulation - which is why the development of interoperability has been recognized by G20 Leaders and is increasingly featured in digital economy agreements.

This report outlines a range of concrete steps that the DCO Member States can take to develop interoperability mechanisms. This includes steps to lay the groundwork for interoperability, such as a common data classification scheme and agreement on principles in areas such as privacy, consumer protection, and national security. In addition to these steps, the report provides a deep dive into interoperability mechanisms that enable cross-border flows of personal data. Such mechanisms can be bilateral, regional, or amongst all DCO Member States and tailored to the DCO Member States' level of ambition and development. The report also looks at how to enable data flows that support cross-border recognition of digital IDs and the international linking of digital payment systems to support DCO Member States' digital economy policies.

The development of interoperability mechanisms is on the global agenda yet remains underdeveloped. Progress by the DCO Members States on the recommendations outlined in this report would demonstrate the opportunity for interoperability mechanisms for supporting economic growth, trade, and innovation and position the DCO General Secretariat and the DCO Member States to take more of a leadership role on these issues.

Glossary and Abbreviations

APEC CBPR	Asia Pacific Economic Cooperation Cross-Border Privacy Rules
APEC PEA	Asia Pacific Economic Cooperation Privacy Enforcement Authorities
ASEAN MCC	Association of Southeast Asian Nations Model Contractual Clauses
BCRs	Binding Corporate Rules
CJEU	Court of Justice of the European Union
CNDP	Morocco's National Commission for the Protection of Personal Data Protection
CPTPP	Comprehensive and Progressive Trans-Pacific Partnership
DEA	Digital Economy Agreement
DFFT	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)
EU GDPR	European Union General Data Protection Regulation
FTA	Free Trade Agreement
G7 Digital Trade Principles	Data should be able to flow freely across borders with trust
ID4D	Nigeria's Digital Identification for Development program
ISO 20022	International Organization for Standardization (ISO) 20022 Universal Financial Message Scheme messaging standards
Malabo Convention	African Union Convention on Cyber Security and Personal Data Protection 2014
NAFTA	North American Free Trade Agreement
OECD Guidelines	Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Trans-Border Flows Personal Data
PSP	Payment System Provider
RECP	Regional Comprehensive Economic Partnership
Schrems II	Ruling of the CJEU affecting businesses transferring personal data outside of European Economic Area
SCCs	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.
USITC	United States International Trade Commission
USMCA	United States-Mexico-Canada Agreement
US-EU Privacy Shield 2.0	The Trans-Atlantic Data Privacy Framework
WTO GATS	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

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. Digital Economy Policy in the Kingdom of Saudi Arabia, https://www.mcit.gov.sa/sites/default/files/digitaleconomypolicy_en.pdf
2. <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>
3. <https://www.jordanvision.jo/en>
4. 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>
5. Digital Pakistan Policy, Ministry of IT and Telecom, http://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf
6. Unlocking Pakistan's Digital Potential" Alpha-Beta, October 2021: <https://alphabeta.com/wp-content/uploads/2021/10/pakistan-digital-transformation.pdf>
7. Kuwait National Development Plan 2020-2025, https://media.gov.kw/assets/img/Ommah22_Awareness/PDF/NewKuwait/Revised%20KNDP%20-%20EN.pdf
8. "Digital Economy," Government, Bahrain, accessed December 15, 2022, <https://www.bahrain.bh/wps/portal/en/BNP/About-TheKingdom/DigitalEconomy>
9. 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>
10. Nigeria Digital Economy Development Department, <https://nitda.gov.ng/department/the-digital-economy-development-department/>
11. Oman Digital Transformation https://oman-portal.gov.om/wps/portal/index/etransformationplan/!ut/p/a1/04_Sj9CPykssy0xPLMn-Mz0vMAfGjzOL9Aw3NDD38DbwtDlydDRydN-P1NTAwdDfxDjYAKIoEKDHAARwNC-sP1o8B-KjA3cDQz8LT19vUN8HQ2MjMPcvCx9zIx-dXEygCvBYEzyap1-QG2GQZeKoCADwbFGg/dl5/d5/L0IKQSEvUUt3RS80RUkhL2Vu/
12. Oman Vision, 2040 https://www.mof.gov.om/pdf/Vision_Documents_En.pdf
13. GlobalData, Mar 2020, <https://www.globaldata.com/media/technology/ict-spending-in-oman-will-reach-us5-6bn-in-2024/>
14. Digital Cyprus Strategy 2020-2025, [https://www.dmridd.gov.cy/dmridd/research.nsf/all/927EA351714F99EDC22587CE-0028C090/\\$file/Digital%20Strategy%202020-2025.pdf?openelement](https://www.dmridd.gov.cy/dmridd/research.nsf/all/927EA351714F99EDC22587CE-0028C090/$file/Digital%20Strategy%202020-2025.pdf?openelement)
15. <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/cyprus-national-digital-strategy-2020-2025>
16. https://add.gov.ma/storage/pdf/Avril_NOG_ADD_fr_SITE_VF.pdf
17. <https://www.bmz-digital.global/en/initiatives/digital-transformation-center-morocco/>
18. <https://www.weforum.org/agenda/2022/07/rwanda-is-tackling-digital-development-challenges-and-succeeding/>
19. <https://www.bloomberg.com/news/articles/2022-04-12/rwanda-looks-to-space-to-boost-information-technology-footprint?leadSource=uverify%20wall>
20. 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
21. https://www.nirida.gov.rw/uploads/tx_dce/National_Strategy_For_Trsansformation_NST1-min.pdf
 22. <https://smex.org/wp-content/uploads/2021/12/The-Digital-ID-Landscape-In-the-GCC-1.pdf>
 23. <https://www.idemia.com/news/kingdom-morocco-launches-national-digital-id-platform-idemia-2022-05-19>
 24. 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/>.
 25. 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>.
 26. "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>.
 27. 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>.
 28. Macdonald, "Nigeria Reaches 90M Digital ID Registrations as Database Capacity Issue Looms."
 29. Burt, "Nigeria's Digital ID Strides Hailed, but More Work Needed to Hit 148M Enrollments by 2024."
 30. Nigeria National Identify Management Commission
 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. 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)
 36. 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
 37. "How AI Can Pump New Life into Oilfields," Expert Insights (IBM, February 2020), <https://www.ibm.com/downloads/cas/5BNKGNLE>.
 38. Memia Fendri, Felipe Bezamat, and Ruben Behaeghe, "The Future of Manufacturing Is Powered by Data and Analytics. Here's Why," World Economic Forum, September 9, 2022, <https://www.weforum.org/agenda/2022/09/manufacturing-data-advanced-analytics/>.
 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.
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. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," Centre for International Governance Innovation, May 10, 2016, <https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization>.
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. 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/>
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>
48. 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>
49. Hosuk Lee-Makiyama, Badri Narayanan, and Simon Lacey, "Cross-Border Data Flows: The Impact of Data Localisation on IoT" (GSMA, January 2021), [https://www.gsma.com/publicpolicy/wp/-Suominen and Vambell. "Alliance for E-Trade Development: Toward an African Data Transfer Regime to Enable MSMEs' Cross-Border E-Commerce" content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf](https://www.gsma.com/publicpolicy/wp/-Suominen and Vambell.)
50. U.S.-Mexico-Canada Trade Agreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors, United States International Trade Commissions, April 2019, Pub. No. 4889
51. Quantifying the Cost of Forced Localization, Leviathan Security Group, accessed December 16, 2022, <https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization>
52. World Bank, World Development Report 2021: Data for Better Lives (The World Bank, 2021), <https://doi.org/10.1596/978-1-4648-1600-0>
53. EU GDPR, <https://gdpr-info.eu/art-2-gdpr/>
54. European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
55. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) (Schrems II).
56. 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/>.
57. 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_72021e35a826441d-b0723642a79e65e5.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
 58. 2021 G7 Digital Trade Principles, <https://www.mofa.go.jp/mofaj/files/100251122.pdf>
 59. 2021 G7 Digital Trade Principles, <https://www.mofa.go.jp/mofaj/files/100251122.pdf>
 60. Cameron F. Kerry, Joshua P. Meltzer, Andrea Renda, Alex Engler, and Rosanna Fanni. “Strengthening International Cooperation on AI,” page 68, Brookings Institution (October 25, 2021). <https://www.brookings.edu/research/strengthening-international-cooperation-on-ai/>.
 61. 2019 Osaka G20 Leader’s Declaration, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html
 62. “G20 Rome Leaders’ Declaration,” European Council, October 31, 2021, <https://www.consilium.europa.eu/en/press/press-releases/2021/10/31/g20-rome-leaders-declaration/>
 63. “G7 Trade Ministers’ Digital Trade Principles,” GOV.UK, October 22, 2021, <https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles>.
 64. WTO GATS Article XIV, https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm
 65. WTO Appellate Body Report, Brazil—Measures Affecting Imports of Retreaded Tyres, 3 December 2007, WT/DS332/AB/R, Appellate Body Report, United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005, para 306–08.
 66. CPTPP Article 14.8 <https://www.cambridge.org/core/books/big-data-and-global-trade-law/uploading-cptpp-and-usmca-provisions-to-the-wtos-digital-trade-negotiations-poses-challenges-for-national-data-regulation/59483E5412CA936C31F6E-BCF9CD97FDF>
 67. 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>
 68. World Bank Development Report 2021, p 190, <https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1600-0>
 69. Amendments to the Personal Data Protection Regulation | um Al-Qura Newspaper, <https://uqn.gov.sa/?p=22736>
 70. “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>.
 71. “What Is Personal Data?,” European Commission, accessed December 16, 2022, <https://commission.europa.eu/law/law-topic/data-protection>

- [ta-protection/reform/what-personal-data_en](#).
72. "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.
 73. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>
 74. <https://www.dataguidance.com/notes/pakistan-data-protection-overview>
 75. <https://www.bahrain.bh/wps/wcm/connect/f84429ee-549e-43ce-b954-8728055f795b/LAW+NO.+%2830%29+OF+2018+WITH+RE-SPECT+TO+PERSONAL+DATA+PROTECTION+LAW.pdf?MOD=AJPERES>
 76. The Law No. 58/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy, <https://www.risa.gov.rw/data-protection-and-privacy-law#:~:text=On%20October%2015th%202021,ensures%20privacy%20of%20individual%20users>.
 77. The Law No. 58/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy Article 3.2, <https://www.risa.gov.rw/data-protection-and-privacy-law#:~:text=On%20October%2015th%202021,ensures%20privacy%20of%20individual%20users>.
 78. Amendments to the Personal Data Protection Regulation | um Al-Qura Newspaper, <https://uqn.gov.sa/?p=22736>
 79. EU General Data Protection Regulation (GDPR), 2016, 679, Article 45, <https://gdpr-info.eu/>
 80. EU General Data Protection Regulation (GDPR), 2016, 679, Article 44.
 81. Schrems v Data Protection Commissioner (2014) I.E.H.C. 310, para 73.
 82. EU General Data Protection Regulation (GDPR), 2016, 679, Article 46.
 83. EU General Data Protection Regulation (GDPR), 2016, 679, Article 47.2.
 84. EU General Data Protection Regulation (GDPR), 2016, 679, Article 47.2(f).
 85. Directive 95/46/EC, European Parliament and the Council of the EU, 1995, Article 7(f); EU General Data Protection Regulation (GDPR), 2016, 679, Article 49.1(h).
 86. APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines (Asia-Pacific Economic Cooperation, 2011), at 10.
 87. "Global Cross-Border Privacy Rules Declaration," U.S. Department of Commerce, accessed December 16, 2022, <https://www.commerce.gov/global-cross-border-privacy-rules-declaration>.
 88. FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework," The White House, October 7, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>
 89. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) (Schrems II).
 90. Wakeman, "Privacy Shield 2.0 —Third Time's the Charm?," Lawfare, May 19, 2022, <https://www.lawfareblog.com/privacy-shield-20%E2%80%86%E2%80%94third-times-charm>.
 91. "FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework," The White House, October 7, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>

- sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.
92. "Statement from U.S. Secretary of Commerce Gina Raimondo on Enhancing Safeguards for United States Signals Intelligence Activities Executive Order," U.S. Department of Commerce, October 7, 2022, <https://www.commerce.gov/news/press-releases/2022/10/statement-us-secretary-commerce-gina-raimondo-enhancing-safeguards>.
 93. "Questions & Answers: EU-U.S. Data Privacy Framework," Text, European Commission - European Commission, October 7, 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.
 94. ASEAN Model Contractual Clauses for Cross Border Data Flows https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf
 95. ASEAN Model Contractual Clauses for Cross Border Data Flows https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf
 96. Macdonald, "Nigeria Reaches 90M Digital ID Registrations as Database Capacity Issue Looms." <https://www.biometricupdate.com/202209/nigeria-reaches-90m-digital-id-registrations-as-database-capacity-issue-looms#:~:text=Nigeria%20reaches%2090M%20digital%20ID%20registrations%20as%20database%20capacity%20issue%20looms,-Sep%2019%2C%202022&text=Nigeria%20officials%20say%20they%20have,crunch%20could%20be%20ahead%2C%20however>.
 97. Burt, "Nigeria's Digital ID Strides Hailed, but More Work Needed to Hit 148M Enrollments by 2024." <https://www.biometricupdate.com/202207/nigerias-digital-id-strides-ailed-but-more-work-needed-to-hit-148m-enrollments-by-2024>
 98. Nigeria National Identity Management Commission, <https://nimc.gov.ng/>



Follow Us on

   @dcorg |  www.dco.org