

Open data

Digital identity

Digital government

Digital public infrastructure

DCO Policy Watch

Navigating the digital policy landscape

Edition 2 | Sep 2024

DCO Policy Watch | Sep 2024

Table of contents

| 1 | Overview | 1 |
|---|-------------------------------------|----|
| 2 | Digital Public Infrastructure (DPI) | 3 |
| 3 | Digital government | 13 |
| 4 | Digital identity | 21 |
| 5 | Open data | 28 |
| 6 | Conclusion | 37 |

1 Overview

Welcome to the second edition of the DCO Policy Watch, a quarterly publication designed to keep policymakers, experts, and decision makers in DCO Member States, Observers, and stakeholders apprised of the evolving landscape in digital policy. This publication serves as a platform for sharing insightful analyses and updates on the latest trends and developments within key areas of digital governance. Our aim is to facilitate a deeper understanding of varied international practices and strategies, thereby supporting our readers in informed decisionmaking and effective policy formulation.

In our first edition issued in May 2024, we delved into the evolving landscape of digital policy, highlighting key trends and recent developments in Artificial Intelligence (AI), Data Protection and Privacy, Electronic Waste (E-waste), and the Future of Work. These discussions provided a foundational understanding of some of the critical issues shaping digital governance and set the stage for our ongoing exploration of the digital ecosystem.

Since our inaugural issue in May 2024, policy developments in the four areas we covered have continued to take place. In AI, several significant developments have taken place, including the launch of a Global Index on Responsible AI in June 2024, the conclusion of the ITU's AI for Good Global Summit 2024 in May 2024, as well as the finalization of the Seoul Declaration, the Seoul Statement of Intent toward International Cooperation on Al Safety Science, and the Frontier Al Safety Commitments at the Second Al Summit in Seoul, also in May 2024.

Additionally, other international organizations and regional bodies have also continued to advance their efforts towards regulating Al. This includes the adoption of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law ("Al Convention") in May 2024 - the first international legally binding treaty of its kind – as well as the Organization for Economic Cooperation and Development's (OECD) updates to its AI Principles, in order to account for new technological developments in the area. The Hiroshima AI Process, initially commenced by the G7, also saw the addition of 49 new countries as part of the Hiroshima Al Process Friends Group. Most recently, in September 2024, The United Nations Secretary General High-Level Advisory Body on AI has released its report "Governing AI for Humanity". The report proposes a framework for global AI governance, emphasizing the critical role of global cooperation, capacity development, and standards.

Regarding global efforts to counter e-waste, in June 2024, OECD updated its rules for the transboundary movement of e-waste, now allowing for greater efforts towards circularity in the management of electrical and electronic waste in its Member States. Additionally, also in June 2024, the European Union (EU) adopted the Right to Repair Directive (R2RD), as well as publishing a new draft of its Waste Shipments Regulation.

Regarding data protection and privacy, in the US, in June and July 2024, the states of Minesota and Rhode Island became the 19th and 20th states respectively to adopt comprehensive data privacy laws. Additionally, in May 2024, a Draft American Privacy Rights Act (APRA) was unanimously approved by a House Committee on Energy and Commerce Subcommittee on Data, Innovation and Commerce.

Finally, AI continues to dominate the conversation around the Future of Work, with the OECD launching a new portal to track this impact in June 2024. Additionally, some tech companies have started to move away from remote work, which started during the COVID-19 pandemic, and introduce return to office mandates.

The second edition of the DCO Policy Watch focuses on the theme of Digital Public Infrastructure (DPI). As the backbone of modern digital economies, DPI encompasses a range of critical digital platforms and systems that facilitate the seamless delivery of services to the public, enhance citizen engagement, and drive economic growth. This edition aims to provide an in-depth examination of three pivotal aspects of DPI: Digital ID, Open Data, and the role of DPI in enabling the Digital Government alongside a brief exploration of the broader impacts that effective DPI systems have on development.

For Digital Government, we explore how governments are leveraging technology to transform public service delivery, improve efficiency, and foster greater transparency and accountability. On Digital Identity, we look at how this has become a cornerstone of secure and inclusive digital economies, and crucial for enabling access to services and ensuring trust in digital interactions. Finally, with Open Data, we will look at government initiatives that are driving a new era of transparency, innovation, and collaboration.

Join us as we delve into these critical aspects of DPI, offering insights, analyses, and case studies to support informed decision-making and effective policy formulation. Together, we aim to advance the collective understanding of DPI and its transformative potential for achieving digital prosperity for all.

For ideas, suggestions, and feedback on this newsletter, please contact:



Digital Public Infrastructure (DPI)

And the Role of Physical Infrastructure and Investments in DPI

2.1 Overview

Digital Public Infrastructure (DPI) has gained significance in the global discussions, with various international organizations and forums emphasizing its critical role in fostering digital transformation, inclusion, and economic growth. The key themes emerging from these discussions include the need for secure, open and interoperable systems, the importance of inclusive and sustainable development, and the vital role of public-private partnerships.

DPI encompasses essential elements such as digital identity, payment systems, and secure data exchange platforms, each playing a vital role in building robust digital public ecosystems. While there have been varying understandings and definitions of DPI, the 2023 G20 New Delhi Leaders' Declaration defines it as:

I a set of shared digital systems that are secure and interoperable, built on open technologies, to deliver equitable access to public and/ or private services at a societal scale. "

DPI can be pivotal in driving development, inclusion, innovation, and trust. With that said, it must be governed by legal frameworks that ensure security, and respect human rights. This has been emphasized in a recent report from the United Nations (UN) Envoy on Technology in April 2024, which states that DPI must adhere to principles of safety, inclusivity, and privacy to build trust and foster development.

Various methodologies from the DCO, European Commission, G20, and OECD provide broader metrics for assessment of impacts of the DPI, focusing on digital skills, infrastructure, business transformation, public services, inclusivity, interoperability, cybersecurity, socio-economic impact, and the effectiveness of governance frameworks. By utilizing comprehensive metrics, policymakers and stakeholders can track progress, identify gaps, and drive improvements in digital public infrastructure to foster sustainable development and economic growth.

The global discourse on DPI underscores its pivotal role in fostering digital inclusion, economic development, and innovation. International organizations and multilateral forums like the UN and G20 highlight the need for secure, interoperable, and inclusive digital systems. The emphasis on public-private partnerships, robust governance frameworks, and the sharing of best practices aims to ensure that DPI benefits all segments of society, driving sustainable and equitable digital transformation. The deployment of DPI by governments involves multiple layers of infrastructure, each critical to building a robust and effective digital ecosystem. This process begins with the physical layer, which includes critical components such as the core Information and Communications Technology (ICT) infrastructure and data centers. The digital layer builds on this foundation, incorporating key elements of DPI like Digital Identity, Payment Systems, and Data Exchange Platforms, which enable the secure and efficient flow of information. The domain layer then integrates sectorspecific solutions, including payment platforms, healthcare systems, and civic registration. Finally, at the top are citizen and business-facing applications, such as electronic passport and visa renewals, online land title registrations, and permit applications, which are key services enabled and facilitated by DPI, making service delivery to the public more accessible, efficient, and secure. <u>A depiction of the various layers</u> within the DPI equation is as follows:

Figure 1: The multi-layered structure of DPI.



Source: https://www.thoughtworks.com/en-au/insights/blog/platforms/digital-public-goods-platform-citizen-services

Robust physical infrastructure, including broadband networks and stable electricity, is fundamental for delivering efficient digital public services. For example, the <u>EU Connecting Europe Facility (CEF-Digital)</u> aims to leverage investments in digital connectivity and has facilitated cross-border interactions and the deployment of free public Wi-Fi through initiatives such as <u>WiFi4EU</u>. Such infrastructure underpins the entire DPI ecosystem, enabling the trusted delivery of public and private services and supporting overall socioeconomic development through digital transformation.

Insightful Publications:

- 1. The UN has been actively involved in promoting DPI to achieve the Sustainable Development Goals (SDGs). In April 2024, the Interim Report on DPI Safeguards, released by the UN Office of the Secretary-General's Envoy on Technology and the UNDP, highlighted the potential of DPI to bridge the digital divide and accelerate progress towards the SDGs. As mentioned earlier, the report emphasizes the importance of trust, safety, and inclusivity in DPI design and implementation. It calls for robust governance frameworks and participatory processes to ensure DPI is used effectively and equitably across different regions and populations.
- The Bill and Melinda Gates Foundation supports DPI initiatives around the world and maintains a <u>helpful</u> <u>webpage</u> illustrating the impact of DPI, success stories, and its work around the world in the area.

3. In May 2024, the <u>UN Environment</u> <u>Programme published a report on Digital</u> <u>Public Infrastructure for Environmental</u> <u>Sustainability</u>. The report examines the information challenges stakeholders face in environmental sustainability decisionmaking and highlights the crucial role of DPI in providing accessible, timely, and credible information, emphasizing the need for both private and public solutions to prevent data fragmentation, and explores six technological innovations in the agri-food sector that can address these challenges.

These include:

- Open data discovery for environmental sustainability.
- Privacy enhancing technologies to enable flow of environmental sustainability information.
- Data markets for environmental sustainability-related data.
- Computational law and data integration of green and circular economy policy measures.
- Using Large Language Models to 'speak' with green and circular economy policy.
- Tools and techniques for humancentered artificial intelligence in environmental sustainability decisionmaking.

2.2 Key trends and developments

Efforts towards advancing DPI have been taking place across all regions of the world. These initiatives are aimed at enhancing digital connectivity, digitally delivered and enabled services, and governance to foster economic growth and societal benefits. The regional developments below highlight high-level work to support DPI in different parts of the world, with specific examples of work on Digital Government, Digital Identity, and Open Data that are highlighted in subsequent sections of this publication.



The policy landscape for DPI in Europe is driven by comprehensive strategies and initiatives aimed at enhancing digital connectivity, services, and governance. To assess the maturity and outcomes of various aspects of DPI, the EU's Digital Economy and Society Index (DESI) tracks digital performance across connectivity, digital skills, internet usage, technology integration, and public services. The <u>EU's Digital Single Market</u> strategy aims to ensure seamless online access and foster a conducive environment for digital networks and services. Some of the key initiatives related to DPI include the EU's e-Government Action Plan, which aims to modernize public administrations and provides interoperable digital services across the EU, as well as the European Data <u>Strategy</u>, which aims to create a single market for data, promoting data-driven innovation while ensuring high standards of privacy and security.

Another important example associated to DPI is the new <u>T2 system</u>, which replaced the TARGET "Trans-European Automated Real-time Gross Settlement Express Transfer System" in 2023. This system is part of the Euro system's consolidated platform for real-time gross settlement and central bank liquidity management. T2 enhances the existing infrastructure by providing more robust and flexible services, critical for supporting the financial stability and efficiency of the Eurozone's e-payment system. By ensuring seamless, secure, and real-time settlement of high-value payments across member states, T2 exemplifies the core elements of DPI, specifically payment systems and secure data exchange platforms. It facilitates the integration of the Eurozone's financial markets. It underscores the importance of interoperable and secure digital systems for delivering public and private services at a societal scale.

National efforts also play a significant role. Estonia's e-governance model, featuring e-Residency, digital ID, and online public services, serves as a good example of DPI ecosystem (see Digital Government section). Germany's Digital Agenda as part of its Digital 2025 Strategy and France's Digital Republic Bill illustrate robust national strategies aimed at fostering digital transformation and inclusive digital public services. In the UK, the government has developed a robust approach to DPI through targeted policies and strategies to enhance public service delivery and ensure digital inclusion. Central to this effort is the Government Digital Service (GDS), and the <u>GDS's</u> 2021-2024 Strategy which oversees the design, implementation, and maintenance of the digital infrastructure supporting government services.



The policy landscape for DPI and the enabling physical infrastructure in North America is driven by strategic initiatives at both federal and state levels aimed at enhancing digital services, connectivity, and security. In the United States, the Federal Communications Commission (FCC) focuses on expanding broadband access through initiatives like the <u>Rural Digital Opportunity</u> Fund, which aims to bridge the digital divide in underserved areas. The National Institute of Standards and Technology (NIST) promotes cybersecurity frameworks essential for DPI. E-government initiatives, such as the US Digital <u>Service</u> and <u>18F</u> (a digital services agency of the US Government that delivers digital services and technology products within the General Services Administration), work to improve digital services' efficiency and accessibility across federal agencies (see Digital Government section).

For payments, the Fedwire Funds Service,

operated by the US Federal Reserve Banks, is a Real-Time Gross Settlement (RTGS) system that enables large-value transfers between banks. It is a critical component of the US financial system, providing the backbone for electronic payments and supporting economic stability.

In **Canada**, the <u>Digital Charter</u> sets the framework for digital transformation, focusing on trust, privacy, and data protection. The <u>Canadian Digital Service (CDS)</u> enhances public service delivery through user-centered design and modern technology. Additionally, <u>Lynx</u> is Canada's new high-value payment system operated by Payments **Canada** under the oversight of the Bank of **Canada**. It replaced the previous Large Value Transfer System (LVTS) in 2021 and provides enhanced security and efficiency for large-value transactions, making it a critical component of Canada's DPI.



The policy landscape for DPI in Latin America (LATAM) focuses on enhancing digital connectivity, services, and governance to promote socioeconomic development. Countries such as **Brazil**, **Mexico**, and **Colombia** are leading in implementing DPI strategies. Some of the key initiatives include Brazil's <u>Gov.br</u> platform, which offers over 4,200 digital services, including digital identity and e-government services, to over 156 million users.

Case Study

Open Finance and Payment System in **Brazil**: The <u>Open Finance initiative</u>, led by the Central Bank of **Brazil**, aims to transform the financial sector by promoting transparency, competition, and innovation. It includes a wide range of financial services and leverages standardized Application Programming Interfaces (APIs) for secure and efficient data sharing, with strict data privacy and security measures to protect consumer information. By enabling third-party providers to access financial data, Open Finance fosters competition, drives digital transformation, and empowers consumers to make informed financial decisions.

Brazil's Open Finance initiative demonstrates the potential of regulatory frameworks and technological infrastructure to reshape the financial landscape. The initiative addresses challenges such as data privacy and consumer trust while offering opportunities for innovation and market competition. Its comprehensive approach provides valuable insights for other countries looking to implement similar initiatives, highlighting the importance of a robust regulatory environment and consumercentric focus.

Beyond the Open Finance Initiative, the Central Bank of **Brazil** also maintains the <u>PIX System</u>, an instant payment system allowing individuals and businesses to make real-time payments through mobile devices, online banking, or ATMs. PIX has become a central part of Brazil's DPI, increasing the use of digital payments.

Furthermore, Mexico's <u>National Digital Strategy</u> aims to provide universal internet access, promote digital government, and enhance digital skills among citizens, and Colombia's <u>Live</u> <u>Digital Plan</u> focuses on expanding broadband infrastructure, improving digital literacy, and fostering a digital economy.



The policy landscape for DPI in the Asia-Pacific (APAC) region is shaped by diverse strategies and initiatives focused on enhancing connectivity, digital services, and innovation. Some higher level initiatives include **Japan**, where the <u>Society 5.0 initiative</u> integrates physical and cyber spaces to create a smart society. In South **Korea**, the <u>Digital New Deal</u> aims to establish

a robust digital economy by investing in data infrastructure, AI, and 5G networks.

In Australia, the Digital Transformation

<u>Strategy</u> focuses on providing seamless online government services, improving digital skills, and ensuring cybersecurity. **Singapore** is another example of the deployment of widescale DPI, with the <u>Smart Nation</u> initiative leveraging digital technologies to enhance public services, urban living, and economic competitiveness (see Digital Government section). In India, the <u>Aadhaar</u> <u>system</u>, part of its <u>Digital India campaign</u>, provides a unique digital identity to over a billion people, facilitating access to various services.

Case Study

The National Database and Registration Authority (NADRA) of Pakistan showcases the power of DPI through its comprehensive digital identity system. Established in 2000, NADRA employs advanced biometric technologies and integrated databases to issue secure Computerized National Identity Cards (CNIC), which enable citizens to access a wide range of e-government services, financial products, and social benefits online. This digital infrastructure has streamlined service delivery, reduced bureaucracy, and enhanced the efficiency of public administration.

NADRA's digital platform has significantly impacted Pakistan's governance and service delivery. It has facilitated financial inclusion by providing digital identities for banking access, improved disaster response through accurate beneficiary identification, and bolstered national security with reliable biometric verification. Despite certain challenges including expanding digital access to remote areas, NADRA's implementation illustrates the transformative potential of DPI in creating a secure, efficient, and inclusive digital ecosystem. As DPI continues to be prioritized, the APAC region has also seen the release of several electronic payments systems by central banks. Some examples include the <u>Raast system</u> launched by the Central Bank of **Pakistan**, India's <u>Unified Payments Interface (UPI)</u> launched by the National Payments Corporation of India (NPCI) under the guidance of the Reserve Bank of India (RBI), and <u>Singapore's Fast and Secure Transfers</u> (FAST) service managed by the Monetary Authority of **Singapore** (MAS), which allows for near-instantaneous interbank transfers 24/7.

Regional cooperation is also evident in some parts of APAC, especially with the <u>ASEAN's Digital</u> <u>Masterplan 2025</u>, which seeks to foster a digitally inclusive community, enhance cybersecurity, and support digital innovation across the ASEAN member states.



Middle East and North Africa (MENA)

The policy landscape for DPI in the Middle East and North Africa (MENA) region is marked by a mix of ambitious national strategies and regional initiatives aimed at fostering digital transformation. Some examples of domestic efforts include the United Arab Emirates (UAE), where the <u>Digital Dubai initiative</u> aims to transform **Dubai** into a smart city through digital services, blockchain, and Al integration.

Additionally, in <u>Saudi Arabia</u>, Vision 2030 includes significant investments in digital infrastructure, emphasizing e-government services, cybersecurity, and digital innovation. This has already been complimented with a range of systems which illustrate the government's work on DPI, for example:

• <u>Absher Platform</u>: Absher is an e-government platform that allows citizens and residents to access a wide range of government services online, such as visa issuance, passport renewal, and traffic violations management, enhancing convenience and reducing the need for physical visits to government offices.

- <u>Saudi Payments (Mada)</u>: Mada is the national payment network that facilitates electronic transactions, supporting the Vision 2030 goal of moving towards a cashless society by promoting the use of digital payments.
- <u>Government Service Bus (GSB)</u>: The GSB is an integrated platform that connects various government entities, enabling seamless data sharing and interoperability, thus improving coordination and efficiency in public service delivery.
- <u>Etimad Platform</u>: Etimad is a digital platform for managing government financial transactions, streamlining budget preparation, contract management, and procurement processes, enhancing transparency and efficiency.
- <u>Yesser e-Government Program</u>: Yesser focuses on developing and implementing e-government services across all government entities, promoting the integration and accessibility of digital services to create a digitally enabled government.
- <u>SADAD</u>: SADAD is the national electronic bill presentment and payment system, streamlining the process of bill payments by providing a centralized platform for various payment services, promoting digital payments and economic efficiency.

Other countries such as Egypt with its <u>Digital</u> <u>Transformation Strategy</u> focuses on building a Digital Egypt by expanding broadband access, developing e-government services, and enhancing digital literacy, and **Qatar**, similarly with the <u>National Vision 2030</u> integrates ICT to improve public services, promote economic diversification, and ensure cybersecurity. Moreover, most countries in the region have either already developed, or are currently developing a comprehensive electronic payments system as a part of their DPI journey. Some examples include the <u>Bahrain Electronic</u> <u>Network for Financial Transactions (BENEFIT)</u> managed by the Central Bank of **Bahrain**, <u>Jordan Mobile Payment (JoMoPay)</u> operated by the Central Bank of **Jordan**, and <u>OmanNet</u> managed by the Central Bank of **Oman**.

Regional cooperation is evident in initiatives like the <u>Arab Digital Economy Strategy</u>, which aims to harmonize digital policies across the region, promoting integration and digital inclusion.



The development of DPI in Africa has seen significant advancements in recent years, driven by the continent's growing recognition of the importance of digital transformation for socio-economic development. Governments across Africa are investing in various DPI initiatives to enhance connectivity, improve public service delivery, and foster economic growth.

Countries such as **Rwanda** and **Nigeria** have made notable progress. Rwanda's <u>Irembo</u> <u>platform</u> provides over 100 e-government services online, streamlining processes and improving access for citizens and businesses. Nigeria's <u>National Identity Management</u> <u>Commission (NIMC)</u> has implemented a digital identity system that supports various public and private services.

With payment systems being a key component of DPI, many African countries have highly developed electronic payments systems in place as their economies go through digitalization. These include the <u>Ghana</u>

Interbank Payment and Settlement Systems

(GhIPSS) operated by the Bank of Ghana, which includes services like the e-Zwich biometric payment system, GhIPSS Instant Pay (GIP), and the national switch, as well as the <u>Real Time Clearing (RTC)</u> system and the <u>South African Multiple Option Settlement</u> (SAMOS) system, managed by the South African Reserve Bank, are foundational to the country's financial infrastructure.

Regional initiatives such as the <u>Smart</u> <u>Africa Alliance</u> are fostering collaboration on digital policies and infrastructure, with projects like the One Africa Network aimed at reducing communication costs and improving connectivity. These efforts are part of the broader <u>African Union's Digital</u> <u>Transformation Strategy for Africa (2020-2030)</u>, which aims to create a unified digital market and promote innovation across the continent. These initiatives collectively aim to bridge the digital divide, enhance public service delivery, and stimulate economic growth across Africa.

The road ahead

Digital infrastructure in general, and DPI in particular is increasingly recognized as a foundational enabler for both public and private sector service delivery. Key actors driving this narrative include international organizations like the UN Development Programme (UNDP), the G20, and the International Telecommunication Union (ITU), among others.

The ITU promotes DPI as an essential element for the digital transformation of cities and countries. It supports the creation of digital networks that enable economic opportunities and public services. The ITU underscores the role of DPI in fostering innovation, competition, and closing gaps in financial inclusion by leveraging digital platforms for services and transactions across both public and private sectors.

Organizations in the private sector and initiatives from civil society like the <u>Gates</u> <u>Foundation</u> and the <u>Carnegie Endowment</u> for International Peace also highlight the importance of DPI. They advocate for interoperable, secure, and inclusive digital infrastructure to support both public services and private sector innovations. DPI is seen as crucial for creating resilient digital economies and improving governance, technology, and market integration globally.

In the public sector, DPI improves healthcare delivery, streamlines social services, and enhances tax compliance etc. In the private sector, DPI facilitates personalized financial services, innovative payment solutions, and improved customer experiences etc. By fostering interoperability and data integration, these systems drive innovation and efficiency, ultimately benefiting citizens and consumers.

Successful DPI generates significant spillovers and benefits across various sectors. It enhances digital inclusion, improves education, fosters greater social and economic inclusion, and promotes digital literacy. These outcomes contribute to broader economic growth and social equity, ultimately leading to more resilient and inclusive societies. The strategic implementation of DPI is crucial for harnessing these benefits and driving sustainable development.

While DPI offers numerous benefits, it also faces several significant limitations and challenges. These include concerns related to sovereignty, privacy and data security, the digital divide and accessibility, regulatory and legal hurdles, interoperability and technical challenges, and sustainable funding and investment. Effective policies, robust regulatory frameworks, significant investment in infrastructure, and a commitment to inclusive and secure digital transformation are necessary to overcome these challenges and fully realize the benefits of DPI.

By leveraging definitions and frameworks from reputable sources like the UN, G20, and OECD, nations and organizations can align their strategies and collaborate on implementing inclusive, secure, and scalable digital infrastructure. These efforts will contribute to a cohesive global approach to digital transformation, ensuring that DPI initiatives are effective, equitable, and sustainable.

Upcoming events

Global DPI Summit 2024

Cairo, Egypt | 1-3 October 2024

Find out more

G20 Leaders' Summit

Rio de Janeiro, Brazil | 18-19 November 2024

Find out more

Internet Governance Forum

Riyadh, Saudi Arabia | 15-19 December 2024

Find out more

Digital Public Infrastructure

across DCO Member States

DCO Member States have dedicated efforts in areas such as Digital Government, Digital Payments, Digital Identity, and Open Data, all of which are highlighted in the subsequent sections. A non-exhaustive list of high-level policies and initiatives relevant to DPI in DCO Member States includes:

| Member State | Initiative | Description | Relevance |
|--------------|--|--|--|
| Bahrain | etraffic App | This application is provided in collaboration with the Ministry of Interior – General Directorate of Traffic (GDT), United Insurance Company, the Ministry of Oil, and the Information and eGovernment Authority to allow users to benefit from services related to driving and traffic. | Digital Government, Digital Identity, Digital Payments |
| Junum | Sehati App | The App makes it easy for users to view their medical information provided by the heath sector in of Bahrain and manage their medical appointments. For example, the Blood Donation Service enables users to register in the blood donation bank, request blood donation, and view medical instructions for blood donations. | Digital Government |
| Greece | Transparency Portal ('Diavgeia') | The Transparency Portal is an internet platform where all government institutions upload their acts and decisions with special attention to issues of national security and sensitive personal data. Following Law 3861/2010 (which established the Portal) and Law 4727/2020 which incorporates relevant European Directives into Greek law, all institutions are obliged to upload their acts and decisions on Diavgeia, as they are not considered valid, unless published. The Portal was upgraded in June 2014 (Diavgeia II), offering a more user-friendly environment, greater accessibility, an open data delivery system, and interconnection with other public systems. | Open Data |
| Jordan | Sanad App | Sanad is a mobile application for digital government services, allowing users to login with a single username and password. Activating Sanad digital identity allows users to access their government digital documents, apply for government and private services, access personal records, digitally sign documents, make bill payments, and others. | Digital Government, Digital Identity |
| Oman | Shifa App | The Shifa application aims to display patients' health data in various health institutions in a streamlined and simple manner from all health institutions affiliated with the Ministry of Health. The application is considered a qualitative leap in the field of digital transformation in the Sultanate. It is a dedicated platform for the health sector that stores medical information and allows exchanges of such information between patients and physicians. | Digital Government |
| Pakistan | Islamabad City App | The Islamabad City App is a multi-feature government service provider application developed for the Islamabad's citizens. It offers more than 40 government services, including ICT services, e-Police, excise and taxation, and utility bills. The app provides a comprehensive suite of tools to enhance the quality of life in Islamabad, including notifications, city guides, utility bill payments, and more. It has been instrumental in improving public service delivery, reducing the need for physical visits to government offices, and promoting a paperless environment. | Digital Government |
| Rwanda | IremboGov | IremboGov is the one-stop portal for e-governance services and is the gateway to Rwandan government services. | Digital Government |
| | Najiz Center | Najiz is a Center for Judicial Services by the Ministry of Justice in partnership with the private sector to provide the Ministry's services under one roof. It saves the client time and effort. | Digital Government |
| Saudi Arabia | Absher platform | Absher is an electronic platform provided by the Ministry of Interior that allows citizens, residents, and visitors to access government services in an integrated and digital manner. | Digital Government |
| | Nafath App | Nafath is a national initiative of the National Information Center to issue and manage citizens' and residents' digital identities similar to the physical ones. The goal is to implement and reinforce the National Digital Identity Strategy governing digital identities. | Digital Identity |

3 Digital Government

The rollout of DPI enables governments to fundamentally transform their interactions with citizens by creating more efficient, transparent, and accessible services. A significant aspect of this transformation is the development of digital government initiatives, which leverage DPI to streamline public administration, improve service delivery, and enhance citizen engagement. By integrating the core elements of DPI including digital identity, payment systems, and data exchange platforms, governments around the world are offering seamless online services such as tax filings, social benefits, healthcare access, and more. This shift not only improves efficiency but also builds trust between governments and citizens, fostering a more inclusive digital society.

3.1 Overview

This section of the DCO Policy Watch explores recent developments, key trends, and the outlook for digital government across different regions, with a focus on DCO Member States towards the end. As governments worldwide recognize the potential of digital technologies to enhance public service delivery, increase efficiency, and foster transparency, we are seeing a diverse range of approaches and strategies emerge.

Digital government initiatives continue to gain momentum globally where countries are at different stages of digital government adoption and maturity. Some examples of countries leading the way in digital government include **Estonia, Canada, Colombia**, and the **Republic of Korea**, countries which scored high in digital government implementation on the <u>OECD's</u> <u>2023 Digital Government Index (DGI)</u>. Within the DCO's ecosystem, most Member States have established national strategies or plans outlining their digital government ambitions, and some have integrated digital government within their long-term national development plans. Major progress on digital-government services has been made over the past few years, especially following the COVID-19 pandemic. However, in some cases, this has not yet translated into a measurable improvement in civic participation, or the quality of public services delivered. Despite the efforts and the known benefits, many countries still lack a well-defined and comprehensive strategy for a shift to digital government. Some of the key challenges include technical barriers such as ICT infrastructure, organizational barriers such as lack of qualified personnel or resistance to change, social barriers such as digital divides, and financial barriers such as lack of budgetary resources.



- Improved service delivery
- Increased transparency and accountability
- Cost savings and operational efficiency
- Citizen engagement and participation
- Data-driven policymaking
- Economic development and innovation



- Digital divide and accessibility
- Privacy concerns
- Legacy systems and interoperability
- Capacity building and skills development
- Cybersecurity risks
- Citizen trust and adoption
- Budgetary resources

Figure 2: The six dimensions of the OECD Digital Government Index



Developments

Great leaps forward in digitalization government services in Jordan:

In June 2024, Jordan reported significant progress, with 55-60% of government services now digitized as part of larger digital transformation efforts.

Find out more

Saudi Arabia launches Digital Transformation Index 2024: In March

2024, Saudi Arabia launched a revised Digital Transformation Index to improve e-government services and innovation, aiming to raise standards for government digitalization.

Find out more

UN Digital Government Awards: In

October 2023, the UN Digital Government Awards 2023 recognized progress in digital public services supporting the Sustainable Development Goals (SDGs), highlighting advancements in countries like Bhutan, Burundi, El Salvador, Togo, and Mexico. The launch of the UN Digital Government Community aims to facilitate knowledge exchange and technology sharing in public service innovation, particularly in developing economies.

Find out more

Digital government offers a powerful avenue for governments to modernize their operations, enhance the quality and efficiency of service delivery, and strengthen transparency and citizen participation. By embracing digital transformation, governments can better meet the evolving needs of their citizens and contribute to sustainable socioeconomic progress. The OECD's Digital Government Index assesses the digital transformation of governments across six key dimensions: digital by design, data-driven public sector, government as a platform, open by default, user-driven, and proactive governance. These dimensions collectively measure how well governments are integrating digital technologies into their operations, promoting transparency, engaging citizens, and providing efficient, user-centered public services. The index serves as a tool for benchmarking and guiding countries in their digital government strategies, helping them to achieve more effective and inclusive governance.

3.2 Key trends and developments

Efforts towards furthering digital government have been taking place in all regions of the world. The UN maintains an E-Government Development Index (EGDI), with global rankings for 2022 (the latest year the study was conducted). This index illustrates Denmark, Finland, and South Korea ranked at the top, showcasing strong performances in online services, telecommunication infrastructure, and human capital. The index also highlighted growing disparities, with many countries in Africa and other developing regions lagging due to limited digital infrastructure and lower investment in e-government initiatives. The report underscored the need for increased focus on digital inclusion and capacity-building to bridge these gaps.



According to the UN, Europe is a global leader in digital government development, with the highest average EGDI value of 0.8305. All European countries have EGDI values above the global average, with 81% classified as very high. The European Commission and EU Member States are advancing cross-border digital public services, contributing to rapid and uniform progress. Europe's success stems from its robust ICT infrastructure and significant human capital investment, essential components of the EGDI. The region excels in providing online services to vulnerable populations and offers a wide array of digital services, reinforcing its global leadership in digital government.

Estonia stands out as one of the frontrunners in European digital government, with a comprehensive digital public services infrastructure based on the Principles of the Estonian Information Policy. Estonia's digitalization strategy includes a widely adopted electronic identification scheme and a secure data exchange platform (X-Road), setting a global benchmark. The Estonian model emphasizes user experience, political support, and data-driven improvement. Despite its success, Estonia faces challenges in citizen engagement, public trust, and cybersecurity threats. The country plans to address the needs of digital nomads, ensuring continued advancement in digital government services.



The US has a well-established federal <u>Digital</u> <u>Government Strategy</u> that was launched in 2012, aiming to build a 21st-century platform to better serve the American people. The strategy's principles are:



Information-Centric: Treat all content as data, ensuring accuracy, availability, and security.

Shared Platform: Promote the use of common standards and architectures to reduce costs and duplication.



Customer-Centric: Focus on the needs of customers, providing accessible, current, and accurate information.



Security and Privacy: Ensure the protection of sensitive government and citizen assets in a rapidly changing technology landscape.

The <u>"21st Century Integrated Digital Experience</u> <u>Act"</u> (21st Century IDEA) of 2018 further mandates federal agencies to annually report progress on modernizing their digital services.

Canada's Digital Government Strategy, known as Canada's Digital Ambition, prioritizes a digital-first approach to enhance public services. Its key strategic themes include modernizing IT systems, leveraging data for improved services, developing actionable digital policies, and enhancing funding, talent, and culture to support digital transformation. Despite being recognized by the OECD for its digital government practices, **Canada** faces challenges such as service consistency and centralized financial reporting. Canada plans to focus its future efforts on securing new digital services, managing aging IT systems, ensuring privacy and transparency, addressing talent shortages, and optimizing IT investment decisions.

Latin America and Caribbean (LAC) countries exhibit varying stages of digital government adoption. Several countries have developed strategies to enhance transparency and efficiency, with some Caribbean nations committing to digitalize public services by 2030. **Colombia**, which the OECD recognizes as one of the best practice countries, passed its <u>Digital Government Policy</u> in 2018, aiming to improve service efficiency, transparency, and quality through a citizen-driven approach. The policy includes strengthening citizen-state digital relationships and improving public entity operations. The region generally is making significant strides, though challenges in implementation and consistency persist.



Sub-Saharan African countries are increasingly embracing digital government, with various nations implementing distinct strategies and initiatives to enhance their digital governance capabilities. Notable efforts include Rwanda's ICT for Governance <u>Cluster Strategy</u> and <u>Irembo platform</u>, which have positioned the country as a leader in e-government. However, challenges such as infrastructure development, digital literacy, and socioeconomic disparities remain prevalent across the region. Countries like Kenya, Nigeria, and Ghana have also launched comprehensive digital transformation plans, aiming to improve service delivery, increase transparency, and drive socio-economic development through technology. Despite the challenges, the region's commitment to digital innovation signals a promising future for e-government in Sub-Saharan Africa.



The MENA region is witnessing substantial growth in digital government initiatives, with countries like the UAE, **Saudi Arabia**, and **Qatar** making significant investments to enhance efficiency, transparency, and service delivery. Many countries are aligning their strategies with the <u>OECD Recommendation on</u> <u>Digital Government Strategies</u>, implementing comprehensive policies to foster digital government transformation. Notable policies include Bahrain's <u>Digital Government Strategy</u> <u>2022</u>, Egypt's <u>ICT 2030 Strategy</u>, and Qatar's <u>2023 NextGen Digital Government Strategy</u>, and the <u>Qatari 2030 Digital Agenda</u> which includes seamless digital government as one of its key pillars.

Saudi Arabia has put large amounts of investment into its digital infrastructure, led by the Digital Government Authority. The country's e-governance platform, <u>Absher</u>, provides over 160 government services to 20 million registered users and is recognized for its extensive features and high security standards. Saudi Arabia's efforts have garnered international recognition, <u>ranking 1st</u> in the UN's Government Electronic and Mobile <u>Services Maturity Index for 2023</u>.



The APAC region shows diverse levels of digital government adoption, with countries like Singapore, the Republic of Korea, and Japan leading globally, while many developing economies are making significant strides in transforming public services. The region's strategies and plans reflect this diversity, ranging from Australia's Data and Digital **Government Strategy to Bangladesh's** e-Government Master Plan for Digital Bangladesh and Fiji's digitalFIJI program. Other notable initiatives include Singapore's Digital Government Blueprint, China's 14th Five-Year Plan for Digital China, and Japan's **Digital Government Action Plan. Countries** like Malaysia, Mongolia, and the Philippines are also advancing their digital government frameworks, emphasizing public sector digitalization and comprehensive e-governance master plans.

The Republic of **Korea** has several ongoing initiatives in this area, with its <u>Digital</u>

Government Master Plan 2021-2025, which

focuses on intelligent public service, databased government, and a strong digital transformation foundation. South Korea's e-governance model, including systems like <u>KONEPS</u> for e-procurement and <u>UNI-PASS</u> for customs clearance, have been recognized globally. The country's approach leverages AI and cloud computing to foster a transparent, people-centered government, enhancing both public services and private sector growth.

3.3 Key trends and developments

Key trends and developments which can be identified from regional initiatives are:

- Comprehensive national strategies: Estonia's <u>Digital Society Development Plan</u> 2030 and Saudi Arabia's <u>Smart Government</u> <u>Strategy</u> exemplify holistic approaches to digital transformation across multiple sectors.
- Focus on emerging technologies: The Republic of Korea's <u>Digital Government</u> <u>Master Plan 2021-2025</u> emphasizes the use of Al and cloud computing for intelligent public services. Singapore's Tech Acceleration Lab program allows both public and private sector entities to prototype digital government products using advanced technologies.
- User-centric approach: Canada's <u>Digital</u> <u>Ambition</u> strategy prioritizes user-centric services that are secure and focused on privacy. Colombia's <u>Digital Government</u> <u>Policy</u> emphasizes a citizen-driven approach in developing remote public services.
- Data governance and interoperability: Estonia's X-Road platform serves as a model for secure data exchange across government agencies and between public and private sector organizations. The EU's efforts towards <u>cross-border digital public</u>

<u>services</u> also highlight the importance of interoperability.

- Cybersecurity and privacy: Saudi Arabia's <u>Digital Experience Maturity Index for</u> <u>Government Services</u> includes security and privacy as key components.
- Digital skills development: The UK's Government Digital Service Strategy for 2021-2024 as well as the Digital Development Strategy 2024-2030 include a focus on building digital capability across government and the digital transformation of government. Rwanda's ICT for Governance Cluster Strategy 2020-2024 aims to expand inclusive government digital services.
- Open government data: The <u>US Digital</u> <u>Government Strategy Milestones</u> emphasizes secure access to digital government information and services anywhere, anytime, on any device; interoperability and openness; and reducing costs. <u>Bahrain's Open Data</u> <u>Portal</u> is another example of this trend.
- Mobile-first strategies: Saudi Arabia's <u>Absher</u> platform, accessible via web and mobile app, exemplifies this approach.

The road ahead

Experts are of the view that digital government offers a major opportunity for governments to modernize their operations, enhance service delivery, increase transparency, and engage citizens. However, to implement it successfully, a comprehensive, well-thought-out strategy is essential, addressing technical, policy, and socioeconomic factors.

The global landscape of digital government policies and initiatives reflects the increasing prioritization of public sector digitalization across countries and regions. Leading digital nations exemplify comprehensive strategies coupled with robust implementation

Upcoming events

Digital Government Africa Summit

Lusaka, Zambia | 2-4 October 2024

Find out more

GovTech Show and Exhibitor 2025 London, UK | 19 March 2025

Find out more

DigiGov Expo London, UK | 20-21 May 2025

Find out more

Transforming UK Public Services Digitally to Deliver Better Outcomes for Communities London, UK | 4 June 2025

Find out more

frameworks, positioning them amongst global best practices. With the EU's concerted efforts for regulatory harmonization, there is a clear recognition that international collaboration is vital for accelerating progress. The future of digital government lies in creating more personalized, efficient, and transparent public services. Key priorities include:

Figure 3: Key Priorities for the Future of Digital Government: Personalized, Efficient, and Transparent Public Services

| Digital Government | 1 Developing future-proof digital infrastructure to support evolving technological needs. | <u>`</u> ` |
|--------------------|---|--|
| | 2: Enhancing cross-border collaboration and knowledge sharing to accelerate digital government maturity globally. | |
| | 3: Addressing digital divides and ensuring inclusive access to digital services, particularly for underserved populations. | |
| | 4: Implementing ethical frameworks for emerging technologies in public sector use, especially concerning AI and data analytics. | |
| | 5: Fostering a culture of innovation and agility within government institutions | |
| | 6: Developing sustainable funding models for long-term digital transformation initiatives. | (Line) (L |
| | 7: Enhancing digital identity systems to enable seamless and secure access to a wide range of government services. | କୁଲୁ ଜୁଲୁ ଅନ୍ଦୁ |
| | 8: Improving data analytics capabilities to enable more data-driven policymaking and service delivery. | |

Digital Government across DCO Member States

DCO Member States are at varying stages of digital government adoption and maturity. This section provides a non-exhaustive list of the digital government policy landscape within the DCO ecosystem.



4 Digital 4 Identity

Digital identity systems are a core element of DPI, serving as a cornerstone for secure and inclusive digital economies. They are crucial for enabling access to services, ensuring trust in digital interactions, and supporting the efficient delivery of public services. Additionally, digital identity plays a vital role in promoting financial inclusion and enhancing personal security.

4.1 Overview

Legal identity is a core human right as recognized by the <u>Universal Declaration of</u> <u>Human Rights article 6, International Covenant</u> <u>on Civil and Political Rights article 16</u> and by <u>Sustainable Development Goal 16.9</u>, which aims to provide "*legal identity for all, including birth registration, by 2030*". Digital identity serves as a crucial enabler in accessing this fundamental right, ensuring that individuals can securely and effectively exercise their legal identity in the digital age.

Legal identity enables people to access basic services, such as health, education, social protection, and justice, as well as to participate in civic and economic activities. However, <u>according</u> to the World Bank, more than one billion people in the world lack any form of legal identity, and many more have identity documents that are not accepted in the digital realm.

Digital identity is not a static concept, but rather a dynamic and contextual one, which depends on the purpose and scope of its use. Depending on the level of assurance and verification required, digital identities can be categorized into different types, such as biometrics, electronic national cards, mobile IDs, or virtual documents:

Biometrics are usually considered as the most secure type of digital identity, as they rely on the physical or behavioral characteristics of a person, such as fingerprints, facial recognition, or iris scans. However, they also raise the most privacy and ethical concerns, as they can be used for surveillance and discrimination.

Electronic national cards are one of the most common types of digital identity, as they are issued by governments and recognized by law as proof of identity and citizenship. However, they may not be interoperable with other systems or countries, and they may exclude people who do not have access to them.

Mobile IDs are considered a convenient type of digital identity, as they use smartphones as a platform for storing and verifying identity credentials. However, they may not be universally accepted or secure, and they may depend on the availability and affordability of mobile devices and networks. Virtual documents are a flexible type of digital identity, as they allow users to create and manage their own digital credentials, such as a mobile driver's license or a verifiable credential. However, they may not be legally valid or trusted by third parties, and they may require a standardized framework for issuing and verifying them.

As the world becomes increasingly digitized, especially after the COVID-19 pandemic, the need for reliable and secure digital identity systems becomes more urgent. Digital identity being a core element of DPI, enabling seamless access to public and private services, plays a crucial role in accessing finance and payments by allowing individuals to securely prove their identity and creditworthiness online. When integrated with other DPI elements such as payment systems and data exchange platforms, digital identity facilitates efficient service delivery, ensuring that public and financial services are both accessible and secure. This interconnectedness within DPI enhances overall functionality and supports inclusive digital ecosystems.

However, all these benefits depend on the trust system that underpins digital identity, which involves proving one's identity, verifying it, and ensuring interoperability with other trusted systems. The concept of digital identity is therefore closely linked with digital trust systems and mechanisms, which require technical, legal, and ethical standards to ensure security, privacy, and inclusion.

4.2 Key trends and developments

Digital identity is a rapidly evolving field, reflecting the growing need for secure, efficient, and accessible identification systems worldwide. According to the <u>World</u> <u>Bank Group</u>, over 90% of countries now use a digital database for identity management, with 65% implementing digital verification or authentication for in-person transactions.

Developments

The European Council approved

the elDAS Regulation: In April 2024, the electronic Identification, Authentication and trust Services (elDAS) Regulation, which aims to harmonize digital identity and trust services in the European Union, was approved by the European Council. The main innovation is the establishment of the "European Digital Identity Wallet" or "EUDI Wallet". This new electronic identification tool enables users to verify their identity and access various public and private services across the EU. Moreover, users can sign documents with qualified electronic signatures and use it for strong customer authentication (SCA) purposes.

Find out more

Australian Parliament passes the

Digital ID Bill: In May 2024, the Digital ID Bill, introduced alongside the Digital ID (Transitional and Consequential Provisions) Bill 2023, was passed by the Australian Parliament. This legislation establishes a voluntary Accreditation Scheme for digital ID service providers, designed to provide more convenient and secure online identity verification for individuals.

Find out more

Around 35% have digital identity solutions for online transactions.

Different approaches to Digital ID implementation include centralized systems with a single identity provider (IDP), federated models with multiple IDPs, and decentralized models using verifiable credentials. These architectures aim to balance security, privacy, and user accessibility while mitigating risks of exclusion and ensuring data protection.



The trend towards Digital ID emphasizes continuous innovation in authentication factors, greater user choice, and a shift from bundled identities to attribute-based identities sourced from various providers. The goal is to place the individual at the center of data sharing, ensuring that digitalization enhances inclusion rather than becoming a barrier.



In the EU, there has been an agenda for promoting the development of a common framework for secure and interoperable electronic identification (eID) and trust services across its Member States, to facilitate cross-border transactions and access to public and private services.

Several EU Member States have launched initiatives and policies to foster the adoption and innovation of digital identity solutions. For example, Estonia's, <u>e-Residency</u> program offers a government-issued digital identity for accessing Estonia's business environment. **Estonia** has

Latest developments

Saudi Ministry Introduces Electronic Verification for Pilgrims: In May 2024,

the Saudi Ministry of Interior introduced a digital identity service for pilgrims with a Hajj visa, as part of the nation's digital transformation efforts aligned with Saudi Vision 2030. This service, created in collaboration with the Ministries of Foreign Affairs and Hajj and Umrah, as well as the Saudi Data and Artificial Intelligence Authority (SDAIA), allows pilgrims to verify their identity electronically via the Absher and Tawakkalna platforms.

Find out more

Vietnam introduced the new digital identity system: In June 2024,

Vietnam introduced Decree 69/2024/ND-CP which is aimed at advancing its digital transformation efforts through "Project 06," which aims to modernize the economy and public services. A key element of this initiative is the new national identity system, encompassing civil registration, digital ID, and authentication. As part of this, Vietnam has introduced draft regulations on electronic identification (e-ID) and authentication, applicable to both foreign and domestic entities involved in registration procedures.

Find out more

adopted a centralized, government-led digital identity system which is centered around its e-Residency and digital ID card, and uses a highly secure, government-issued PKI (Public Key Infrastructure) to provide broad access to e-services.

Similarly, Germany's <u>nPA (neuer Personalausweis)</u> national identity card includes a chip for online authentication and electronic signatures. More recently, the **UK** has been developing the '<u>One</u> <u>Login for Government</u>' system, which aims to streamline access to public services by providing a unified digital identity for all citizens. Additionally, countries like **Finland** and **Belgium** have implemented advanced digital ID systems, further demonstrating the widespread adoption across Europe.



Asia-Pacific (APAC):

The digital identity policy area in the Asia-Pacific (APAC) region is characterized by diverse and dynamic developments, reflecting the different economic, social, and political contexts of the countries.

Many countries in the region have initiated or expanded their national identity programs, such as India's <u>Aadhaar</u>, Indonesia's <u>e-KTP</u>, Pakistan's <u>NADRA</u>, and the Philippines' <u>PhilSys</u>, Vietnam's <u>VNeID</u>, Singapore's <u>SingPass</u>, Malaysia's <u>My</u> <u>Identity</u> and Thailand's <u>The Digital ID framework</u> to provide universal and verifiable identification for their citizens.

Countries like **India** and **Singapore** have taken an inclusive approach. India's Aadhaar system is a vast, biometrics-based national identity program, primarily focusing on financial inclusion and public service access for a diverse population. Singapore's SingPass is more focused on integrating everyday governmental and private services into a single, user-friendly digital ID platform, using mobile authentication to simplify access. In addition to national initiatives, some regional and sub-regional cooperation efforts have emerged to foster dialogue and collaboration on digital identity issues among different stakeholders, such as governments, private sector, civil society, and international organizations. For instance, the <u>ASEAN Digital</u> <u>Integration Framework</u> provides a common vision and guiding principles for the development of digital ID systems.



The **United States** adopts a decentralized method for digital identity legislation. Although there are federal guidelines like the <u>NIST Special Publication</u> <u>800-63 Digital Identity Guidelines</u>, there is no unified federal digital identity policy or framework. Instead, the **US** depends on a mix of State and sector-specific laws and regulations to develop digital identity policies. As such, the **US** does not have a unified national digital ID framework, relying instead on state-specific and sectorspecific regulations.

Canada has also been developing a national digital identity strategy based on the principles of privacy, security, interoperability and user-centricity. The <u>Pan-Canadian Trust Framework</u> (PCTF) is a key component of this strategy, as it provides a set of standards and guidelines for verifying the trustworthiness of digital identity services and networks.



The MENA region exhibits a range of digital identity developments, from emerging frameworks to advanced systems leveraging cutting-edge technologies. Saudi Arabia's <u>Absher</u> platform, launched in 2015, uses secure web and mobile technologies, integrating multifactor authentication (MFA) and biometrics to facilitate over 200 government services, such as passport renewals and traffic fine payments.

<u>UAE PASS</u>, employs biometric authentication, digital signatures, and blockchain technology to ensure secure, immutable transactions across both government and private sectors. This platform supports various services, including healthcare, banking, and utility management, enabling users to access these services through a single, unified digital identity. **Qatar** <u>Digital identity (QDI)</u>, similarly, uses advanced cryptographic techniques and biometric verification to provide secure access to a range of services. This system is designed to link digital identities to a wide array of government services, enhancing security and efficiency.

These digital identity systems in the MENA region streamline access to services and reflect a strategic embrace of advanced technologies such as biometrics, blockchain, and cryptography to ensure the security and effectiveness of digital interactions. As these systems continue to evolve, they will play an important role in the region's digital transformation, supporting both national and regional goals for modernizing government and private sector interactions.



Sub-Saharan Africa

Digital identity policies in sub-Saharan Africa are evolving as different countries move forward with their programs in order to provide their populations with reliable and verifiable identification methods. A study <u>estimated</u> that digital identity could generate up to 6% of GDP growth in Africa by 2030, by reducing transaction costs, increasing efficiency, and creating new markets and opportunities. For example, Ghana's National Identification Authority (NIA) is rolling out the <u>Ghana Card</u> <u>project</u>, a biometric smart card that uses fingerprint and facial recognition technology. This multi-purpose card is designed to serve as a secure identification method across various sectors, including banking, healthcare, and voting.

Additionally, Kenya's <u>Huduma Namba</u> project is a centralized digital identity system that assigns a unique personal identification number (PIN) to every citizen and resident, based on biometric and demographic data. This system uses biometric technologies like fingerprints and iris scans to ensure secure and accurate identity verification across government services, including social benefits and healthcare.

Both projects highlight the region's commitment to using digital identity systems to drive socioeconomic development and enhance access to essential services, while also addressing challenges such as identity fraud and inclusion.

The road ahead

As mentioned in the DCO's Digital Economy <u>Trends report</u>, digital identity is key part of modernizing public services and is the cornerstone of access management, authentication, and authorization, facilitating a safe and secure online environment and enabling essential cybersecurity and data protection measures. Therefore, digital identity is a foundational requirement for digital government, as it enables the establishment of trust mechanisms between the government and the citizens. This trust mechanism can be enhanced by the private sector's involvement, but not substituted, as providing and digitizing a citizen identity is the fundamental role of the government.

Looking ahead, the COVID-19 pandemic has highlighted the global relevance of accelerated digital identity requirements. With the rise of digital payments, globalization, and digitization, there is no turning back to physical-only forms of documentation, such as paper or identification cards. Nations that capitalize on the early advantages of digital identity will become early innovators and adopters of trusted and interoperable digital identity solutions. With ongoing elections in multiple countries in 2024 and issues such as deepfakes and disinformation, governments must be proactive in ensuring their citizens feel safe and heard.

One of the key challenges for the future of digital identity policy is to ensure that the principles of privacy, security, inclusion, and innovation are respected and balanced across different jurisdictions and sectors. The emergence of decentralized and self-sovereign identity solutions, which give users more control over their own data and credentials. poses new questions for regulators and policymakers on how to establish credible standards and interoperable systems, as well as protect users from potential risks and harms. Moreover, the increased use of biometric and behavioral data for authentication and verification purposes raises ethical and social concerns about the potential misuse or abuse of such sensitive information if they fall into the wrong hands.

Therefore, it is crucial for stakeholders involved in the digital identity ecosystem including governments, the private sector, civil society, and academia to collaborate and coordinate their efforts to develop and implement effective and responsible digital identity policies. These efforts are essential to fostering trust, inclusion, and innovation in the digital economy and are integral to building and strengthening DPI on a global scale.

Upcoming events

Identity Week Asia 2024

Singapore | 22-23 October 202

Find out more

Think Digital Identity and Cybersecurity for Government London, UK | 24 October 2024

Find out more

Digital identity policies and strategies across DCO Member States

Digital identity systems are being developed across the DCO ecosystem. A non-exhaustive list of digital identity policies and systems in DCO Member States includes:



5 Open Data

Data is a vital resource that powers the the digital economy. Unlocking the full potential of data is critical to enabling a data-driven digital economy. This involves promoting evidence-based decision-making through improved data access, maximizing the benefits of cross-border data flows by aligning governance policies and regulations, and tapping into the wealth of public sector information to strengthen government-citizen interactions. Open Data policies play a key role in achieving these goals.

Open Data, particularly Open Government Data (OGD), is a core element of DPI. OGD involves making government datasets freely available, promoting transparency, innovation, and efficient service delivery. Open data portals are integral to DPI.

5.1 Overview

Open data, according to the <u>Open Knowledge</u> <u>Foundation</u>, refers to <u>"data that can be</u> <u>freely used, re-used and redistributed by</u> <u>all – subject, at most, to the requirement to</u> <u>attribute and share alike.</u>" A key element of open data is its interoperability, enabling various datasets to be accessed and utilized by various organizations for different purposes.

Open Government Data (OGD) enables seamless integration across systems, allowing data from different public sources to be combined and used for public services. For example, open data in transportation networks facilitates real-time applications that improve urban mobility, as seen in Helsinki's public transit system. Open Data portals not only improve service delivery but also empower citizens and businesses by providing the tools needed to innovate and participate in the digital economy.

Open Data stakeholders are categorized into four key advocacy groups: civil society and academia, the private sector, national governments, and multilateral organizations. Civil society and academic organizations promote open data to enhance social equity and economic opportunity. The private sector contributes through initiatives such as Foundation Twenty-Nine's HealthData 29 project supported by Microsoft, and Google's COVID-19 Open Data Repository, aligning with their corporate missions. National governments drive OGD to enhance transparency and improve public service delivery. Multilateral organizations collaborate with governments to compile and share large datasets that underpin global initiatives.

In order to assess the openness of data, several organizations have proposed principles or criteria, that include:

- <u>The International Open Data Charter</u>, which was founded in 2015 and adopted by 27 governments from all regions, including Europe, Africa, and LATAM. This is a set of principles and best practices that guide governments on how to release open data to the public.
- 2. <u>The FAIR principles</u>, which advocate for the Findability, Accessibility, Interoperability and Reuse of digital assets; and
- 3. <u>The Open Definition</u>, which defines "openness" of data and content, which means "anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)."

The <u>key characteristics of an Open Data Portal</u>, as per the EU-financed Open Universal Science (OPUS) project, are captured in the figure below:

These suggest that all Open Data should have characteristics associated to availability and access, reuse and redistribution, universal participation, timeliness and completeness, quality and accuracy, metadata and documentation, standards and interoperability, and privacy and security.

OGD plays a vital role in DPI by enabling datadriven decision-making and improving public service coordination. As more governments adopt open data policies, the potential for innovative solutions in sectors such as healthcare, education, and transportation continues to grow. However, challenges remain, including the need to protect personal data, ensure data quality, and promote the widespread adoption of open data standards.



Figure 4: Key Characteristics of an Open Data Portal

5.2 Key trends and developments

Recent developments in open data policies are shaped by the economic potential that open data harbors, as a crucial commodity within the digital economy. Consequently, there is growing demand by businesses and entrepreneurs to access and leverage this data, as governments strive to ensure data protection and digital literacy are equally developed in tandem with, if not ahead of, open data policies. Within every geographical region, there are examples of nations who have prioritized the development of their open data policies and platforms and started to reap the rewards, and of those who have more recently turned their attention towards this area.



The European Union's Open Data Directive is regarded as a cornerstone of the European open data strategy, having come into force in 2019 and bolstered by the addition of the concept of high-value data sets in 2022. This policy is committed to fair competition and transparency and aims to create a common European market for government-held data. EU Member States were consequently tasked with transposing this policy into their national law by July 2021, with four countries facing late to no transposition infringement procedures. Building on the General Data Protection Regulation (GDPR) and Data Governance Act, this Open Data Directive is testament to the EU's commitment to steering, coordinating and tracking data governance across the region.

Key points of EU the policy include:

- Encouraging EU countries to make as much information available for reuse as possible.
- Stimulating the publishing of dynamic data and the use of APIs.

Latest developments

EU Open Data Directive: In June 2024, the European Commission Implementing Regulation came into force, complementing the EU Open Data Directive. The Commission set out a list of six topic areas in which the reuse of high-value datasets ought to be ensured to maximize the their socioeconomic benefits. These are geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, and mobility.

Find out more

GSA launches Open Government Federal Advisory Committee (OG

FAC): In April 2024, the US General Services Administration (GSA) announced plans to create an OG FAC and invite nominations for membership. This committee will support the GSA in creating, implementing and monitoring open government initiatives.

Find out more

OECD OURdata Index: In December 2023, the OECD issued the findings of the 4th edition of the OECD Open, Useable and Reusable data (OURdata) Index for 2023. This Index serves as a key public governance indicator and indicates the progress made by governments in leveraging open data to support policy reform.

Find out more

- Focusing on written texts, databases, audio files, and film fragments, but not applying to educational, scientific, and research data.
- Covering data held by public sector bodies at all levels, including ministries, state agencies, and municipalities, as well as content held by museums, libraries, and archives.
- Limiting the exceptions that allow public bodies to charge more than the marginal costs of dissemination for the re-use of their data.
- <u>Enlarging the scope</u> to include data held by public undertakings and research data resulting from public funding, with specific rules for re-use and charges.

Beyond the European Union, there are notable developments such as the establishment of national data portals in the **UK** and **Switzerland**, for which the datasets are regularly expanded and updated. Additionally, whilst Lichenstein's open data policy is still under development, data is already easily accessible for the public.

The European Data Portal (EDP) is a key resource that conducts an annual benchmark assessment of open data across the continent. The 2023 report encompassed 35 countries, and the average maturity score stood at 79% overall, and at 83% for EU countries, both increasing marginally from the previous year.



Open data policy formulation and implementation are growing priorities across the APAC region, with nations reaching significant milestones. **Bangladesh** and **Nepal** have both established national open data portals, with **Bangladesh** further advancing by releasing a comprehensive <u>Open Data Strategy</u>. **Pakistan**, Mongolia, and **Sri Lanka** are in the process of developing their open data policies, focusing on enhancing transparency, fostering innovation, and supporting economic growth through greater data accessibility.

Several APAC countries have benefited from preexisting data privacy regulations in shaping their open data policies. For example, **China** and **India** are investing heavily in mapping national policy networks and data ecosystems. This strategic focus will enable both nations to implement open data strategies more consistently at the national level and fully harness the economic potential of open data. These efforts are crucial in ensuring that open data initiatives align with broader OGD frameworks and integrate into their DPI, driving both governance and economic development.

In addition to these initiatives, countries like **Australia**, **Malaysia**, **Korea**, and **Japan** have developed advanced open data policies, supported by comprehensive platforms or portals with extensive data sets. These nations have set ambitious timelines, often spanning three years or more, within their strategies. Their policies not only prioritize data availability and interoperability but also incorporate strong governance mechanisms, data privacy safeguards, and ethical guidelines to ensure responsible data use.

Case study

Korea's OGD Journey: Korea's Open Government Data (OGD) initiative, rooted in the <u>2013 "Act on Promotion of the Provision</u> <u>and Use of Public Data,"</u> has established the country as a leader in digital transparency and innovation. The central <u>Public Data Portal</u> (<u>data.go.kr</u>) provides access to over 80,000 datasets across various sectors, including transportation and healthcare. A key feature of Korea's OGD approach is its emphasis on data quality, ensured through the Public Data Quality Management System, which mandates regular audits and adherence to

strict standards. This initiative has led to significant innovations, such as real-time transit apps like "Seoul Bus" and "Kakao Metro," and has been important in the country's effective COVID-19 response, where open access to health data enabled the development of apps that supported public health efforts.

By linking these open data policies with broader DPI initiatives, APAC countries are enhancing service delivery and citizen engagement, and positioning themselves to leverage the economic benefits of open data. This alignment with OGD and DPI efforts demonstrates a commitment to building resilient and inclusive digital economies while simultaneously addressing the critical issues of data privacy, security, and ethical data use.



Across the Americas, there are varying levels of development and implementation of open data policies. Beyond ensuring governments have sufficient data policies in place, there is recognition of the need to provide guality data for these open data regimes.

Canada ranked highly in the OECD 2023 report and its open data policy, Open Government, illustrates Canada's commitment to enhancing transparency, accountability, and citizen engagement. Canada's high ranking is attributed to its robust open government policies, which emphasize transparency, accountability, and citizen engagement. The policies are further supported by strong legal frameworks and tools, such as the Open Government Portal and the Directive on Open Government which support the proactive release of high-quality data, and the active involvement of stakeholders in the open data ecosystem.

In the **US**, the development of open data polices consists of a federal approach and a state-led approach, resulting in an uneven development of policymaking. The Federal Data Strategy and the ten-year vision it entails, sit alongside state policy. The Federal Government maintains Data. <u>Gov</u> as its open data portal, with most states also having their own open data portals. The <u>Software</u> Alliance (BSA) includes a useful tracker on the maturity of open data policies, though has not been updated since 2022.

Within Latin America, the development of open data polices is still in the relatively early stages and varies greatly across the region. The Open Government Data Policies of Brazil, Colombia, **Uruguay**, and **Argentina** illustrate growing momentum to promote the availability and use of open data, as others focus efforts on developing their data policies, before moving to develop their approaches to open data. Likewise, there is variation in policy development across the Caribbean: Jamaica and the Dominican Republic have both launched open data portals and Haiti became the first country in the region to release budget data.



Middle East and North Africa (MENA)

There are various open data initiatives in the MENA region, including in Saudi Arabia, the UAE, Qatar, Oman and Jordan, who have developed open data policies, portals, and platforms, contributing to the trend of data democratization and a culture of data confidence and data sharing.

Saudi Arabia's national open data portal was launched by the Saudi Data and Artificial Intelligence Authority (SDAIA). This portal provides access to a wide range of datasets across various sectors, including healthcare, environment, and transportation. For example, the healthcare datasets have been instrumental in driving research and innovation, particularly during the COVID-19 pandemic, where real-time data on infection rates and vaccine distribution played a critical role in the country's response. The portal also supports the government's <u>Vision</u> <u>2030</u> by promoting transparency and citizen engagement, thus fostering a culture of datadriven decision-making.

The UAE's open data initiatives are led by the <u>UAE</u> <u>Government Portal</u>, which offers comprehensive datasets spanning sectors such as education, economy, and infrastructure. The portal aims to enhance public access to government data, which in turn supports innovation and efficient service delivery. For instance, in the transportation sector, open data has been used to optimize public transit routes and improve traffic management systems in cities like **Dubai** and **Abu Dhabi**.

In **Qatar**, open data efforts are centered around the <u>National Open Data Policy</u>, which mandates the sharing of government data with the public to promote transparency and innovation. The policy is supported by the <u>Qatar Open Data</u> <u>Portal</u>, which provides access to datasets from various ministries, including finance, health, and education. A key example is the finance sector, where open data on government spending and budget allocations has been made available to enhance transparency and public trust. This initiative is part of Qatar's broader strategy to diversify its economy and promote sustainable development through data-driven policies.

Similar examples exist in **Oman**, with the <u>Oman National Open Data Portal</u>, launched by the National Center for Statistics and Information, which provides access to a variety of datasets, with a focus on economic, social, and environmental data. One notable example is the publication of environmental data, which has been used to monitor and manage natural resources more effectively, contributing to the country's environmental sustainability goals. Several other MENA nations have deployed similar open data portals to accomplish their digital transformation goals and guide decision making through OGD. Some nations are still in the process of developing their open data policies and have more nascent data portals. The development and implementation of open data policies is a key tool to overcome the historical overreliance of some in the region on third party data and insufficient data regimes.

🌍 Sub-Saharan Africa

In cooperation with the international nonprofit organization, <u>Local Development</u> <u>Research Institute (LDRI)</u>, the <u>African Open</u> <u>Data Network</u> seeks to implement programs and conduct research to support socioeconomic development through data sharing initiatives and co-ordinate regional efforts in this aim. The <u>2022 African Union's data</u> <u>policy framework</u> emphasizes the importance of open data standards and principles of open governance and equally, as well as the accessibility of data to entrepreneurs, innovators and researchers.

African Nations have reached various levels in the development and implementation of open data policies. Botswana is focused on developing its open data strategy, whereas others are prioritizing the enactment of data protection laws and enhancing training on data governance. Angola and Benin have both launched national portals, and the efficiency of these portals is largely impacted by the size of the datasets made available. The large dataset of the Kenyan Open Data Initiative supports the national portal and progress has been driven by the 2023-2027 open government partnership action plan. South Africa National Policy on Data and Cloud has also been key in driving the creation of a robust data economy and the growth of the ICT sector.

The road ahead

Open data platforms, as essential components of DPI, will continue to play a critical role in enabling efficient service provision to the public. By facilitating the free access and interoperability of government datasets, these platforms allow for seamless integration across various sectors, enabling more efficient coordination and delivery of public services. As governments expand their open data initiatives, these platforms will serve as the backbone for emerging technologies such as AI, IoT, and Big Data, helping to improve decision-making, transparency, and innovation.

Moreover, the accessibility of open data through these platforms will enable governments to respond more effectively to public needs by streamlining services in areas like healthcare, transportation, and education. As open data policies initiatives evolve, these platforms will ensure that citizens and businesses alike can leverage valuable data, driving further digital innovation and enhancing the overall quality of services to the public

Open data platforms and policies are recognized as a vital component in the delivery of ICT-based applications and services in the DCO's Digital Economy Trends report, for example in the construction of interconnected digitized cities across the globe. The development and deployment of data-centric emerging technologies, such as Internet of Things, Big Data, and AI reaffirms the centrality of data in the digital economy. As Al awareness has grown, so has the need for governance structures, commitments to transparency, and a code of ethics. In this way, open data emerges as an established solution and open data policies are a tool to build trust and confidence among users and encourage cross-sectoral and cross-regional data sharing.

A survey conducted by the <u>Open Data Policy Lab</u> forecasted data stagnancy throughout 2024 –

Upcoming events

UK Open Technology Conference

London, UK | 4-5 February 2025

Find out more

Data Conference 2025

London, UK | 13 March 2025

Find out more

EU Open Data Days

Luxembourg & Online | 19-20 March 2025

Find out more

World Data Summit

Amsterdam, The Netherlands | 21-23 May 2025

Find out more

openness is set to advance, but at a slow rate. In contrast to the trend where commercial data ecosystems are becoming more closed, there is more openness across the public sector, most likely influenced by the evolution of data privacy literacy and related legislation coming out of Europe.

There is a notable move towards open data globally to provide public sector Large Language Models with data to train AI models. The innovative opportunities provided by the intersection of open data and AI is illustrated by the Indian <u>Avyantar Health Technologies</u>, which built a machine learning-powered prediction platform to facilitate the early diagnosis of neonatal sepsis. Additionally, the Guatemalan <u>Afindidata</u> uses AI to create a chatbot and provide parents of young children with smart healthcare and nutrition assistance, and even suggest educational activities. In this way, the Open Data x AI approach may accelerate the open data push as civil society and the private sector look to their governments to make this data readily available and accessible.

For open data to be leveraged in this way by emerging technologies, it is imperative that governments develop and implement the policies, platforms, portals, and datasets that make up the key digital infrastructure that enable open data to safely and securely facilitate these innovations. Nations will seek to strengthen their data policies more broadly, with a focus on data privacy and security, and in doing so, lay the groundwork for data regulation.

The usefulness of such policies and platforms is dependent on the development of comprehensive, transparent datasets to facilitate their operation. Countries like **Angola**, **Algeria**, and **Egypt** have invested recently in the digital infrastructure required to make a national portal, although effectiveness could be compromised by limited availability of quality datasets. There is also demand for access to open government data from businesses and entrepreneurs in LAC countries. It is expected that this demand will accelerate the development and implementation of open data policies and the provision of datasets to launch national portals or platforms in this region.

Open data policies across DCO Member States

Different DCO Member States have different type of open data schemes in place. A non-exhaustive list of these is as follows:



6 Conclusion

This edition of the DCO Policy Watch outlines the key components of DPI and their critical roles in fostering digital transformation, inclusion, and economic growth. DPI is foundational in creating resilient digital ecosystems that support efficient service delivery to the public, promote transparency, and drive innovation. The various elements discussed, such as digital Identity, open data, and an ecosystem of digital governance, are not just isolated components but are deeply interconnected, collectively contributing to a robust DPI framework and its outcomes.

These components, alongside others such as electronic payment systems, systems that support e-health, among others, underpin modern digital economies. Each component plays a unique role in enhancing the efficiency, transparency, and inclusivity of public and private service delivery, ultimately driving socioeconomic development.

Digital government initiatives leverage technology to transform public service delivery, making it more efficient, transparent, and citizen centric. Building these services on top of a robust DPI, governments can ensure that they meet the evolving needs of their citizens in a secure and scalable manner.

Digital identity systems are crucial for ensuring secure access to services and fostering trust in digital interactions. As the cornerstone of a secure and inclusive digital economy, digital identity not only facilitates access to public services but also plays a vital role in promoting financial inclusion and enhancing personal security.

Open data, especially OGD initiatives promote transparency and innovation by making government data freely accessible. By enabling data-driven decision-making, open data enhances public service delivery and fosters greater collaboration between the public and private sectors.

Together, these elements form a comprehensive DPI that supports the seamless integration of technology into public and private governance. This integrated approach improves the efficiency and reach of public and private services and lays the groundwork for sustained digital transformation. As governments continue to build and refine their DPI, the focus should remain on ensuring that these systems are inclusive, secure, interoperable, and capable of evolving with the changing digital landscape. This will ultimately contribute to the creation of resilient and prosperous digital societies that can effectively meet the challenges and opportunities of the 21st century.

Document Disclaimer

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User. The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.





www.dco.org