DATA PRACTICES IN MENA

Case Study: Opportunities and Challenges in Jordan

Findings of a Data Ecosystem Assessment

March 2021

MENA TECH

Unlocking Digital Transformation

AN INITIATIVE OF

WORLD BANK GROUP

Acknowledgments

This report was prepared by a World Bank team, co-led by Adele Barzelay (Governance Analyst, Governance Practice) and Zaki B. Khoury (Senior Digital Development Specialist, Digital Development Global Practice); with input from Jerome Bezzina (Senior Digital Economy Specialist, Digital Development Global Practice), Issa Mahasneh (Consultant), and Suhail Shersad (Consultant). Valuable field support was provided by Nadine Al Rayyan (Consultant).

Additional contributions were provided by Onur Ozlu (Senior Economist, Finance Competitiveness, and Innovation Practice), Marolla Haddad (Digital Development specialist, Digital Development Global Practice) and Fatimah Alotaibi (Consultant). The Country Management Unit provided extensive guidance and field support; the team would like to thank Ali Abukumail (Senior Private Sector Specialist) with the Finance, Competitiveness, and Innovation team for their support in making the mission in Amman successful.

Peer review comments were provided by James Neumann, Tim Kelly, Huong Tran, Craig Hammer, and Andrea Barone as part of a Quality Enhancement Review. Additional comments on the data ecosystem assessment tool were provided by the MNA Tech Data Governance Advisory Council, including Craig Hammer, Vijayanti Desai, Fadilla Caillaud, Cem Dener, Robert Palacios, and Benu Bidani.

Finally, this diagnostic was conducted with support from and in close coordination with Jordan's Ministry of Digital Economy and Entrepreneurship, with close support from Eng. Abdelkader Albatayneh (Director Policies & Strategies, MoDEE) and Ms. Nada Khater (Head of E-government Strategies, MoDEE).

Cover image © passion artist/Shutterstock.com. Icon on Page 6 made by Pixel perfect from www.flaticon.com

Disclaimer

1818 H Street NW, Washington DC 20433 | Telephone: 202-473-1000 | Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Rights and Permissions

Contents

Figures

Tables

Boxes

List of acronyms

AI	Artificial Intelligence
AFR	Africa region
API	Application Programming Interface
ATI	Access to Information
BI	Business Intelligence
CA	Certificate Authorities
CBJ	Central Bank of Jordan
CC-BY	Creative Commons Attribution License
CERT	Computer Emergency Response Team
CLOUD	Clarifying Lawful Overseas Use of Data Act
COVID-19	Coronavirus Disease 2019
CSV	Comma-Separated Values
CTO	Chief Technology Officer
DNL	Department of National Library
DOS	Department of Statistics
DPA	Data Protection Authority
EGDI	E-Government Development Index
EHS	Electronic Health Solutions
ESCWA	United Nations Economic and Social Commission for Western Asia
Fintech	Financial technology
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPR	EU General Data Protection Regulation
GoJ	Government of Jordan
GPC	Government Private Cloud
GSB	Government Service Bus
HCI	Human Capital Index
HPC	High-performance computers
IaaS	Infrastructure as a Service
INTAJ	Information and Communications Association of Jordan
ICT	Information and Communications Technology
ID	Identification
IOT	Internet of Things
JIC	Jordan Investment Commission
JADI	Jeddah, Amman, Damascus, Istanbul Cable Network
JAF	Jordan Army Forces
JEPCo	Jordanian Electric Power Company
JO-CERT	Jordan Computer Emergency Response Team
JUST	Jordan University of Science and Technology
LOB	Legislation and Opinion Bureau
MENA	Middle East and North Africa
ML	Machine Learning
MNA	Middle East and North Africa region
MoDEE	Ministry of Digital Economy and Entrepreneurship
MoICT	Ministry of Information and Communication Technology
MOPIC	Ministry of Planning and International Cooperation
MOU	Memorandum of Understanding
NAF	National Aid Fund
NBN	National Broadband Network

NCC	National Cybersecurity Center
NCP	National Cybersecurity Programme
NCHR	National Center for Human Rights
NIS	National Information Systems
NITC	National Information Technology Center
NLP	Neuro-Linguistic Programming
NUR	National Unified Registry
OECD	Organization for Economic Cooperation and Development
OGP	Open Government Partnership
OSI	Online Services Index
PaaS	Platform as a Service
PPP	Public Private Partnerships
PSUT	Princess Sumaya University for Technology
RCN	Regional Cable Network
SaaS	Software as a Service
SEA	South East Asia region
SGN	Secure Government Network
SME	Small and Medium Enterprises
SOA	Service Oriented Architecture
STEM	Science, Technology, Engineering and Mathematics
TII	Telecommunications Infrastructure Index
TRC	Telecommunications Regulatory Commission
UAE	United Arab Emirates
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
URI	Uniform Resource Identifier

MENA Tech Initiative's Data Governance Activity: Definition and Purpose

There is currently a proliferation of data typologies. A distinction can be drawn between "raw" data and data as information.[1] The scope of data can be broadened to include both data and metadata (machine understandable information about web resources or other things).[2] Data can be differentiated according to the source, that is, distinguishing between public and private sector data and information. Alternatively, data can be classified according to their purpose, irrespective of the collection instrument or the entity managing the data: "public intent data" being data collected for public purposes, versus "private intent data", i.e. data collected by the private sector for commercial purposes.[3] Data can also be defined in relation to its access, on a spectrum from closed to open. Finally, personal data protection regimes are often based on the distinction between personal and nonpersonal data. Within personal data, a distinction is sometimes made between volunteered, observed and inferred data.[4]

Data governance is a necessary process of managing the availability, usability, integrity and security of data in public and private systems. This is usually based on an identified set of data standards and policies that also guide data usage. The process includes strengthening the institutional, regulatory, capacity and technical foundations to better control and manage the data value cycle – that is, the collection, generation, storing, securing, processing, sharing and reusing of data, as means to enhance trust and deliver value.[5]

The MENA Tech Initiative aims to promote effective data governance. There is a need to govern the use and reuse of data for value creation, in both the public and private sectors as well as by civil society. In this vein, data "governance" includes three key pillars: a) enabling and safeguarding policies, laws and regulations; b) hard and soft infrastructure including broadband, interoperability and portability; and c) institutions that enable effective implementation and enforcement of the policies, laws and regulations that promote trusted data usage.[6] It remains critical for governments to foster public trust in the responsible use of data by developing robust and effectively enforced legal and regulatory mechanisms to protect the fundamental rights of data subjects in their personal data, ensure the integrity and security of data, and create incentives for the sharing/pooling of private sector data for public good.

Building trustworthy data governance systems enables the effective harnessing of data for social and economic development. By successfully implementing a robust data governance framework on top of an adequate digital infrastructure, governments in the MENA region will create an enabling environment for the development of an inclusive, safe, innovative and dynamic digital economy. This also sends an important signal of accountability and transparency to incentivize individuals, civil society organizations and businesses to trust the public and private platforms and services whose development responds to user needs and generates value.

The responsible implementation of data governance standards also support countries' aspirations to become competitive actors in the digital economy. It paves the way for the establishment of common data environment principles and the foundation of integrated regional digital markets. For more information, see the **Appendix**.

[1] OECD, "Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies". 2019. Available at: https://www.oecd-ilibrary.org/sites/276aaca8-en/index.html?itemId=/content/publication/276aaca8-en. See also World Bank, World Development Report (2021)

[2] Definition available at https://www.w3.org/DesignIssues/Metadata.html. According to the W3C, "Data will not be discoverable or reusable by anyone other than the publisher if insufficient metadata is provided. Metadata provides additional information that helps data consumers better understand the meaning of data, its structure, and to clarify other issues, such as rights and license terms, the organization that generated the data, data quality, data access methods and the update schedule of datasets."

[3] The distinction between "public intent" and "private intent" has been coined and developed in the World Development Report 2021: Data for Better lives (forthcoming, March 2021).

[4] WEF (World Economic Forum) and Bain & Company Inc. 2011. Personal Data: The Emergence of a New Asset Class. Geneva, Switzerland: WEF. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[5] OECD, "Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies". 2019. Available at: https://www.oecd-ilibrary.org/sites/276aaca8-en/index.html?itemId=/content/publication/276aaca8-en.

[6] This framework is aligned with the conceptual framework for "data governance layers" developed in the World Development Report 2021 that is structured around four "enablers and safeguards" (infrastructure policies, laws and regulations, economic policies and institutions). It is adapted slightly in this activity to align with the priority outcomes of the MNA Tech Initiative and the regional context.

Box 0.1: Harnessing Data for Better Policy-Making

The application of digital technologies has the potential to reshape existing policies, enable innovative policy design and expand citizen engagement in local and national policy-making.

Data can be used to increase the efficiency of targeting and implementation of existing policies, as well as piloting new policies. In agriculture, for example, remote sensing and digital land parcel identification systems allow countries to grant direct subsidies to farmers and to enforce other regulatory measures related to the sustainability of agriculture. In cities, digital cameras that automatically register the license plate of vehicles entering a congestion zone have made it more feasible to design, implement and enforce congestion pricing schemes.

Digital transformation can reshape government-citizen interaction and expand stakeholder engagement. Many countries are making more data freely available to enhance accountability in the public sector and allow for evaluating the effects of current policies. For instance, with publicly available pollutant release and transfer registers online, civil society oversight of regulated entities can be facilitated, enhancing the transparency of compliance efforts and breaches.

Source: OECD (2019)

Executive Summary

Jordan aspires to become a regional digital leader and has identified digital economy as a high priority for the country's social and economic development.[1] With limited natural resources, a digital economy would enable Jordan to diversify its economic activities and migrate to a data-driven economy. Jordan has been one of the earliest to boost digital transformation in the Middle East and North Africa region, including developing the digital infrastructure market and starting the implementation of open government and open data initiatives. However, with the global rise in digital economic transformation, Jordan needs to speed up its initiatives to keep pace with regional and global emerging economies. More recently, the COVID-19 crisis has created an urgency for Jordan to adapt to the post-pandemic world driven by digital infrastructure and services.[2]

Against this background, this case study provides an assessment of the data governance practices in Jordan as well as a set of high-level policy recommendations to strengthen data governance in support of a vibrant, safe and inclusive digital economy. Data Governance is a necessary process of managing the availability, usability, integrity and security of data in public and private systems. Strengthening the data governance ecosystem thus requires developing the underlying infrastructure and implementing a trustworthy management system for the data value-chain: collection, processing, storage and sharing. A solid data governance ecosystem, supported by capacity building for institutions and inclusive communications and dissemination campaigns, can foster trust in data use in a country and region with a fragile social contract.[3]

The diagnostic toolkit used in this report interrogates three pillars:

- **Enablers:** Does Jordan have an adequate data infrastructure, including policies and technical architecture, to enable the collection, storage, sharing, analysis and management of data for value creation?

- **Safeguards:** Has Jordan established trust in the use of data? Does Jordan have the needed safeguards to promote trust in personal data protection and security?

- **Value Creation:** Have the first two pillars (Enablers and Safeguards) facilitated increased use and reuse of data? Have they created data innovation and increased usage of digital services?

The findings of this analysis are mixed.

Enabling data policies and infrastructure

Data infrastructure is a prerequisite for processing, storage and connectivity in digitally enabled public and private processes. Effective infrastructure must include high-quality broadband networks, high-performance computers, data storage and management capabilities (such as cloud based). This "hard" infrastructure must work in tandem with "soft" institutional components such as robust interoperability practices, data portals and platforms, and "access to information" policies to ensure prolific data generation, use and exchange.

[1] In 2016 the government launched "REACH2025: Jordan's Digital Economy Action Plan" with a vision to "have a digital economy that empowers people, sectors and businesses to raise productivity and ensure growth and prosperity, creating a highly attractive business destination for investments and international partnerships." In the Mashreq digital forum held in Amman in June 2019, The Government of Jordan (GOJ) has also committed to advancing the digital economy as strategic growth sector for the Kingdom through improving broadband and cashless payment adoption.

[2] Jordan's prime minister H.E. Dr. Bisher Al Khasawneh's statement on the new Government's program delivered to the Parliament first week of January noted: "Digital transformation: implementation of the "Jordanian Strategy for Digital Transformation" and its roadmap with the aim of enhancing e-government services has a focus on citizens' priorities in vital sectors that directly affect their lives (e.g. health, education, transportation), including the utilization of digital services to promote integrity, combat financial and administrative corruption."

[3] The strengthening of the social contract has been identified as one of the priority objectives of the digital transformation agenda under the MNA Tech Initiative 2.0.

There has been recent progress in governmental openness with deployment of Jordan's Open Government Data platform.[4] **But Jordan's broadband connectivity, cloud services and interoperability policies need scaling up.** The broadband infrastructure is reasonably reliable at present (World Bank 2018), although initiatives to reduce regional and income disparities and lay the groundwork for future-proof technologies should be completed without delay, despite the strains of the COVID-19 crisis. Jordan has had a National Cloud Policy since July 2020 and utilizes a Government Private Cloud to link over 100 public entities. However, there remains great untapped potential to scale cloud infrastructure, especially by the private telecom providers. Impediments to the seamless storage and management of data could be eliminated if interoperability and adherence to unified standards were mandated even as

To scale up data infrastructure, Jordan could implement these high-impact policy interventions:

- Continue investing in modern data infrastructure (e.g., Cloud, 5G and IoT) to maintain forward momentum and ensure that advanced digital applications (e.g., AI-enabled) run smoothly in the future.
- Further develop the national cloud initiative (G-Cloud) to unlock the value of big data and foster scientific and technological innovation.
- Expand authentication through digital identification and enhance open data portals and platforms to improve digital services and e-government.
- Adopt revisions to the Access to Information law[5] to increase transparency and proactive disclosure of public sector information holdings to nongovernment stakeholders.
- Develop and fine-tune regulatory frameworks and standards to support data interoperability and reuse between various government agencies and entities.

Safeguards for fostering trust in data processing and use

Jordan's data governance strategy can be described as a "hybrid" approach to building safeguards. It strikes a balance among exploiting opportunities for data use, protecting individuals' rights in their personal data, and ensuring the integrity and security of sensitive public sector data. Elements of the legal regime are relatively robust (for example the law governing electronic transactions[6] or the cyber-security regime[7]). However, uneven implementation or enforcement jeopardizes the development of a trusted environment for data use. In other areas, such as personal data protection and consumer protection, the legal regime has shortcomings or requires adaptation to be fit for the digital age.

The most urgent priority for the GoJ to enable the trusted use of personal data is to adopt its long-awaited personal data protection law. A draft law from the Ministry of Digital Economy and Entrepreneurship (MoDEE) is currently under review ahead of its presentation to the Parliament. The draft law overall is well aligned with the European Union's General Data Protection Regulation (GDPR), with which it seeks compatibility. However, critical areas of the draft are vague or depart from the GDPR and other international good practice instruments. Explicit clarification of the lawful bases for data processing, other than with informed consent, is especially important in data use cases where consent may be difficult or infeasible to obtain. The draft law also departs from good practice by proposing a multi-stakeholder Data Privacy Board within the MoDEE, rather than establishing an independent authority with clear staffing criteria. Certain clarifications on the regime for cross-border transfers would further support predictability and compliance.

Jordan does not have a specific law for online consumer protection. and would benefit from the extension of its existing consumer protection regime to e-commerce transactions as this area continues to expand rapidly.

Jordan's Cybersecurity Law of 2019 provides additional safeguards to the existing policy framework. though its recent adoption limits the team's ability to assess if it has been implemented and enforced effectively.

[4] https://portal.jordan.gov.jo/wps/portal/OpenData?lang=en&isFromLangChange=yes#/manageDataSets

[5] Law No.47 of 2007 Guaranteeing the Right to Obtain Information. Official Gazette No. 4831, 4142. June 17, 2007.

[6] E-transactions Law No. 15 of 2015. https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/bec70415-2845-42df-bc47-5e0ee4b859b7.pdf

[7] Cybersecurity Law No. 16 of 2019.

To strengthen these policy, legal and regulatory safeguards the GoJ could focus on these high-impact areas:

- Prioritize the drafting and adoption of a data protection law aligned with good practice to enable high-trust processing of personally identifiable information.
- Develop a national data governance framework and strengthen the leadership and coordination of the data governance agenda with input from civil society and the private sector, support consultative and multi-stakeholder implementation of policies, laws, regulations and standards.
- Adopt a whole-of-government approach to the development and implementation of data governance frameworks to manage and use public sector data more effectively.

Unlocking the potential value of data creation

Jordan has been successful in adopting or planning forward-looking data policies.[8] However, for data usage to attain substantial economic value, the key challenge will be to ensure effective and timely policy implementation. Data transfer between public entities, as well as private sector sharing and usage of government data in accordance with applicable legal and regulatory environment, are often nascent and inconsistent across institutions, with limited government-to-business data collaboration. Civil society, universities and research institutions also have limited access to data, with relatively low usage of the datasets on Jordan's open data portal. The disconnect between the supply of public sector data and its use by business and civil society signals a disconnect between accessibility and usability. This may be a function of differences in prioritization criteria, quality or relevance to end users.

Opportunities exist to improve the data infrastructure and increase usage. Notable signs of Jordan's potential for developing high value data include the existence of a small but growing number of private sector companies that specialize in processing government data for corporate data mining. On the public sector side, the GoJ has successfully digitalized key government services, as exemplified by the Ministry of Justice's digitization of case law and the Ministry of Health's automation of a large proportion of medical files. Jordan is ranked 118 out of 193 countries on the UN e-Government Development Index (UN DESA 2020a), and there are significant opportunities to further improve its online services and e-participation applications. The Government's ongoing digital initiatives, including fintech, have high scalability potential, thanks to efforts by the Central Bank and related institutions. These and other sectoral transformations still in preparation make appealing cases for private-public collaboration to generate greater societal value in the future.

Data governance remains an evolving landscape, requiring stakeholder flexibility and dynamism to develop principle-based and technology neutral laws and regulations. Effective implementation requires capable, well-resourced and (where appropriate) independent government institutions, established private sector players, innovative startups, empowered individuals and civil society organizations. The evolution of these stakeholders and data governance practices in Jordan illustrate the opportunities and challenges in enabling socioeconomic value to be created from trusted data use. Mitigating the challenges and exploiting the opportunities requires a long-term strategic vision which balances security and data protection on the one hand with user-centric enablers on the other, at the forefront of the data governance agenda in Jordan.

To enable more effective data governance, three areas of focus are proposed for Jordan. These three areas are based on the recognition that there already is a reasonably robust foundational policy and regulatory framework in place, but standards have not been consistently harmonized and adopted across the whole government, creating challenges for data users.

[8] Jordan has been a regional leader on Open Data, and its draft data protection law includes the right to data portability.

Table ES.1: Areas of focus for Jordan

Data-related challenges to be addressed	Short-term (1-12 months)	Medium-term (12-24 months)	Long-term (24-36 months)
1. **Government data infrastructure limitations** (e.g., architecture; G-Cloud; API standards; network security; etc.)	Finalize adoption of a national cloud policy with clear security standards and certification	Adopt a national government interoperability plan. Address infrastructure investment required to achieve 2030 target.	Develop a new "smart government" strategy that is user-centric and data-driven. Expand Implementation of data infrastructure required.
2. **Limited adoption and/or enforcement of key legislative and regulatory frameworks** enabling trusted data use and sharing	Adopt a revised Data Protection and Privacy Law to regulate the collection and processing of personal data (including by Government) in line with international good practice	Adoption of implementing regulations for the data protection law	Enhance the independence and capability of a data protection agency to support enforcement of the data protection law (guide and clarify standards, enforce, monitor, and provide redress)
3. Weak organizational and institutional **leadership, coordination, and capabilities**	Adoption and implementation of unified standards for classification, sharing and usage of datasets. Enhance the human capital and skills needed in the public sector to implement data-related policies.	Binding policy or regulation defining standards and governing usage of metadata, anonymized data and tagged data (e.g., geo-locations) across the whole-of-government.	Policies and Regulations that enable government entities to securely transfer data across borders and use of processing in secured Data warehouses.

1. Towards a Digital Transformation in Jordan

Digital Transformation in Jordan

Jordan has identified digital transformation as a high priority for the country's social and economic development. The national long-term vision and strategy document, *REACH2025* (MoIT and INT@J 2016), defined a set of initiatives and key performance indicators (KPIs) for both e-Government and the information and communication technologies (ICT) sector, aiming to introduce "Smart Government" and upgrade the country's broadband infrastructure. REACH2025's vision is to "have a digital economy that empowers people, sectors and businesses to raise productivity and ensure growth and prosperity, creating a highly attractive business destination for investments and international partnerships." This initiative was projected to increase digital economy sector revenues by 25% to 30%, and total GDP by an additional 3% to 4%.

The "General Policy for the Telecommunications, Information Technology and Postal Sectors" (MoIT 2018) emphasized the need to move forward in Digital Transformation. According to the policy, the Government should design an effective governance model with clear roles and responsibilities for Digital Transformation, by involving all parties and by enhancing citizen engagement and cooperation with the private sector. This digital transformation program was entrusted to a new ministry established in 2019, announced after a cabinet reshuffle – the Ministry of Digital Economy and Entrepreneurship (MoDEE). But all government ministries and public sector bodies are included in the effort. The policy also calls for the adoption of technology standards and interoperability, while stressing the importance of the relevant skills by creating a Digital Transformation Skills Centre in each public entity.

Jordan's roadmap for digital transformation was reiterated in June 2019 in Amman, at the launch of the Digital Economy and Entrepreneurship Development in Mashreq Forum, organized jointly with the World Bank Group (World Bank 2019). There Jordan's Government committed to developing access to broadband internet for 100% of the population by 2021 and opening the country's existing broadband network (consisting of 7,000 kilometers of optical fiber) for Public-Private Partnership. Other commitments related to increasing nationwide digital (cashless) payments and launching a national skills development initiative.

MoDEE then launched the Jordan Digital Transformation Strategy 2020 (MoDEE 2020a). The mandate of the former Ministry of Information and Communication Technology (MoICT) was thereby expanded to support digital entrepreneurship, digital platforms and digital skills development. The strategy calls for the adoption of a common Data Architecture for governmental agencies to allow interoperability and to support Business Intelligence (BI), data analysis and Big Data. The strategy also includes creation of a National Central Registry, a unified national database with single measures for data classification, to allow data harmonization between public entities.

The data economy provides Jordan with significant opportunities. If a supportive ecosystem can be created, Jordan's various economic sectors will benefit from data as an asset. Contributing about 12 percent of GDP, ICT in Jordan has developed into one of the leading sectors in the region, with more than 600 active companies directly employing about 16,000 employees and contributing about 84,000 jobs in the wider economy (Jordan Investment Commission 2020). This sector can drive further creation of innovative products and services.

Jordan is building a data economy to unleash its potential. While data is becoming ubiquitous in today's economy, the models for governing data are still not working as well as they should. In order to succeed in the next phase of global digital transformation, governments and companies must ensure that data is used in ways that benefit the economy and society. Jordan is not an exception, as the development of digital technologies opens the door to new approaches to data management at the government level, the publication of regulations and policies around data. The GoJ aims to ensure its economy can achieve more by safeguarding the ability of innovators, entrepreneurs and service providers to collect, share and use data in trusted ways.

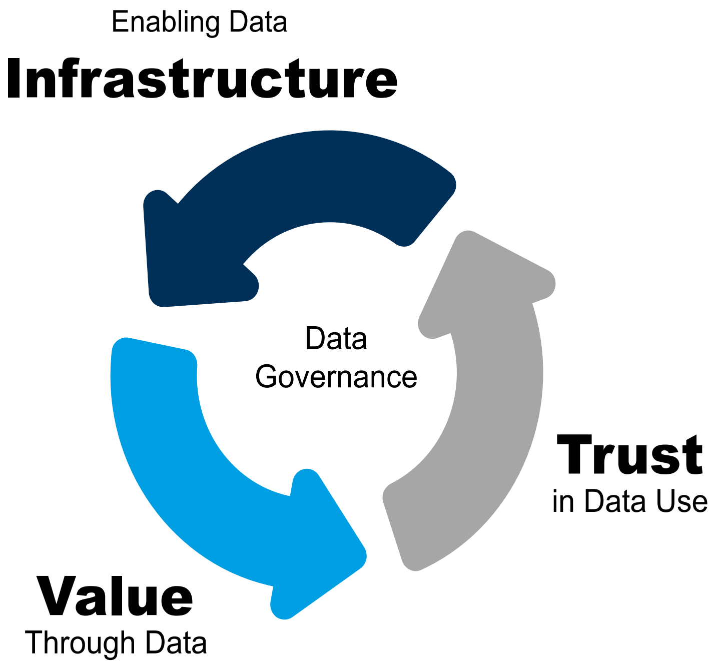
Objectives of this report

This report examines how Jordan is establishing effective and safe value-creating data governance. The aim is to ensure that the way in which data is generated, managed, analyzed and used will eventually maximize the development impact, evolve a nascent digital economy and advance digital transformation. A vibrant, inclusive and safe digital economy can only be enabled by implementing a robust data governance framework on top of an adequate digital infrastructure, and only if individuals, organizations and businesses all have trust in the use of data by putting in place several safeguards. In addition to elaborating an overview of the existing data governance practices in Jordan, and how they interconnect with Jordan's objectives in digital transformation, this case study seeks to highlight emerging challenges, gaps and opportunities. A set of policy recommendations is also offered to support effective data governance in Jordan.

This report utilizes the MENA Tech Initiative's draft diagnostic toolkit, which seeks to characterize three "pillars" of the data economy:

- **Enablers:** Does Jordan have an adequate data infrastructure, including policies and technical architecture, to enable the collection, storage, sharing, analysis and management of data for value creation?
- **Safeguards:** Has Jordan established trust in the use of data? Does Jordan have the needed safeguards to promote trust in personal data protection and security?
- **Value-Creation:** Do the identified enablers and safeguards support and protect the value of personal and business data? Do they foster innovation and increased usage of digital services?

Figure 1.1. Data ecosystem



Source: World Bank.

2. Analysis of the Elements of Data Governance in Jordan

Enabling Data Infrastructure and Complements

Reliable and future-proof digital infrastructure is the foundation for Jordan's data-enabled digital transformation. Data flows rely first and foremost on long-lasting digital infrastructure that can cater to the growing need for speed, security and bandwidth for government, business, academia and individual usage. Building a competitive data and knowledge economy in Jordan will require an effective data infrastructure that depends among other things on:

- high-speed broadband connectivity to transport data (Connectivity);
- world-class data infrastructure to store and manage data (Cloud); and
- powerful high-performance computers (HPC) to process data.

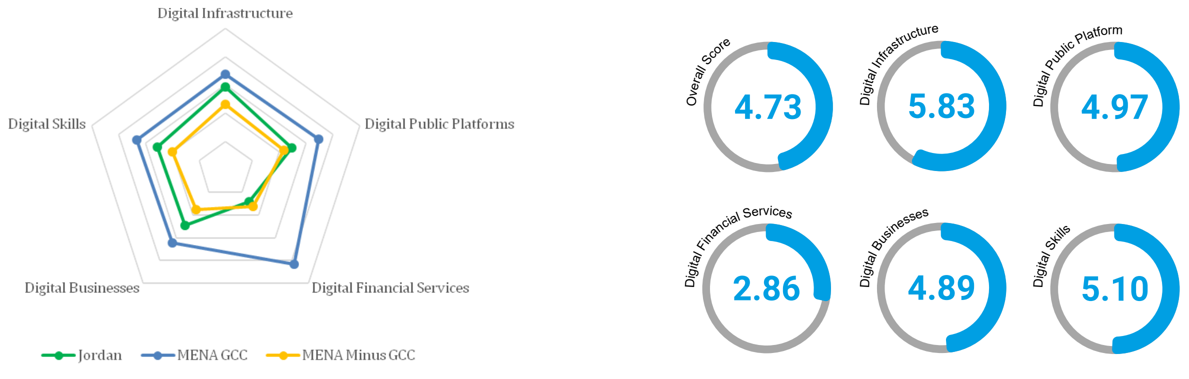
In addition to such "hard" infrastructure, "soft" infrastructure includes data interoperability strategies and policies, technical standards for data classification and management. Additional analog complements necessary to support the effective implementation of data governance frameworks include robust institutional arrangements with appropriate leadership and coordination mechanisms, and a sufficiently resourced, skilled and capable workforce and user base.

Broadband Connectivity

Jordan has a set of challenges and opportunities regarding broadband infrastructure.[1] The country has relatively low scores compared to its regional peers in infrastructure (i.e., fixed broadband infrastructure) and individual usage (also fixed broadband services) but is one of the best in political and regulatory environment and government usage. Jordan ranks 73rd out of 121 countries on the 2019 Network Readiness Index, well ahead Tunisia (84th), Lebanon (86th), Morocco (87th) and Egypt (92nd).   However, the country remains behind the countries of the Gulf Cooperation Council (GCC) including UAE (29th), Bahrain (40th) and Saudi Arabia (45th).

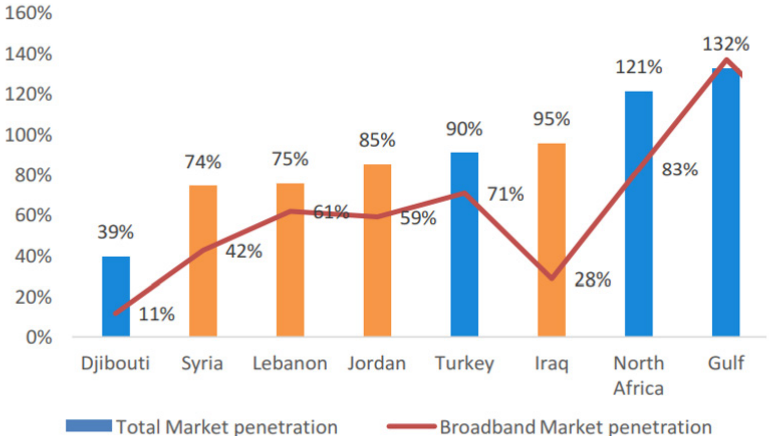
Mobile broadband services are the most used platforms in Jordan. In 2017, 59% of the population had mobile broadband subscriptions. Data shows that there is a gap between the adoption of basic mobile services and mobile broadband services. Due to this gap, Jordan lags behind some regional peers in GCC countries which have penetration rates above 90% for mobile broadband (Figure 2.1). It has also been observed that the gender gap in mobile ownership is 21% in Jordan, while this gap is only 2% in countries like Egypt or Turkey (World Bank 2018).

Chart illustrating Jordan progress on the key pillars of Digital Economy (MNA Tech Dashboard, 2019)



[1] Jordan has secured its international connectivity since 1999. This was established through the port city of Aqaba with the 27,300-km long FLAG submarine cable. Terrestrial alternatives are also available through Amman's interconnection with two major terrestrial fiber optic networks running through the region including the Regional Cable Network (RCN) and the Jeddah, Amman, Damascus, Istanbul (JADI) line, which are not fully functional given the political instability and the various wars in the region.

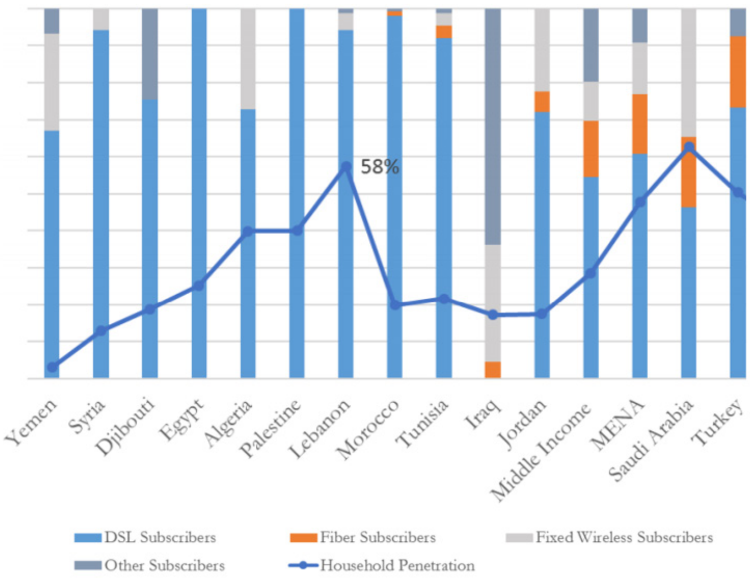
Figure 2.1: Penetration of mobile and mobile broadband services (per 100 inhabitants)



Source: GSMA 2018

Jordan exhibits a low penetration of fiber-based access infrastructure, as most fixed broadband is based on asymmetric digital subscriber line (ADSL) and fixed wireless technologies. Fiber infrastructure is essential for high speed data sharing and the exchange of information. The country has fixed broadband penetration significantly lower than the middle-income countries' and MENA countries' averages (Figure 2.2).

Figure 2.2: Distribution of Fixed Broadband subscriptions by connection technology (%)

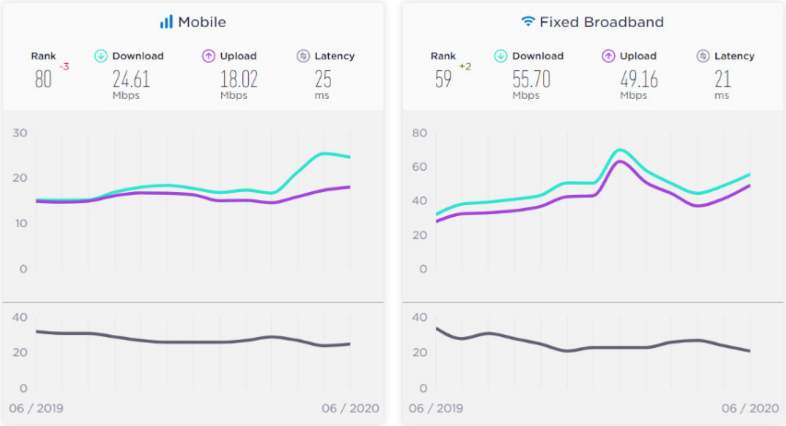


Source: World Bank 2018

Jordan has also limited speed of broadband services when compared to other fast-growing economies in the MENA region, particularly in the GCC countries. According to Speedtest Global Index[2], Jordan ranks 80th in download speed over mobile networks. As for the fixed download speeds, the country ranks 59th out of 134 (Figure 2.3). These constraints inhibit the full potential usage of data generated in or exchanged through the Kingdom (Figure 2.4).

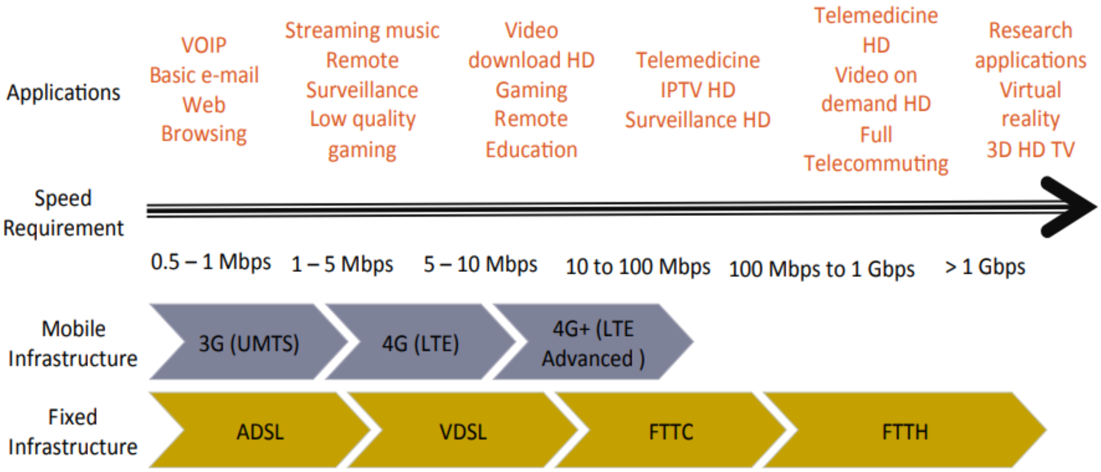
[2] https://www.speedtest.net/global-index

Figure 2.3: Mobile and Fixed Broadband Speed (June 2020)



Source: Speedtest Global Index 2020

Figure 2.4: Broadband speed requirement by application


Applications
VOIP Basic e-mail Web Browsing
Streaming music Remote Surveillance Low quality gaming
Video download HD Gaming Remote Education
Telemedicine IPTV HD Surveillance HD
Telemedicine HD Video on demand HD Full Telecommuting
Research applications Virtual reality 3D HD TV
Speed Requirement
0.5 – 1 Mbps
1 – 5 Mbps
5 – 10 Mbps
10 to 100 Mbps
100 Mbps to 1 Gbps
> 1 Gbps
Mobile Infrastructure
3G (UMTS)
4G (LTE)
4G+ (LTE Advanced)
Fixed Infrastructure
ADSL
VDSL
FTTC
FTTH

Source: World Bank.2018

A transition to 5G services in Jordan is unlikely in the near future as 3G or 4G networks are still developing and the priority is to scale penetration. Jordan's current plan is to deploy 5G services by 2023. The deployment of 5G is expected to connect people, things, data, applications, transport systems and cities in smart networked communication environments[3]. The Telecommunications Regulatory Commission (TRC) has invited operators to conduct trials (Jordan Times 2019) and consultations with key stakeholders to ensure that the appropriate policy and regulatory incentives are adopted to develop the infrastructure required for 5G deployment. The development of a trusted environment and the appropriate data infrastructure will be crucial to incentivize and enable the widespread usage of 5G infrastructure and services which will generate a wealth of important and sensitive data.

At the core of Jordan's broadband infrastructure is the National Broadband Network (NBN). This is a 2,400-km fiber-optic, open access data network connecting more than 1,300 sites across Jordan, including 633 public schools, 8 universities, 23 knowledge stations, 127 government entities and 88 healthcare centers. The Government initiated the project in 2016 with the view to provide high-speed broadband access (100 Mbps) and bandwidth capacity. The

[3] 5G networks can transport a significant amount of data much faster, reliably connect an extremely large number of devices and process very high volumes of data with minimal delay, according to ITU (2020).

aim is to increase universal access and coverage as well as contribute to the efficient and effective development of the country's e-services delivery, quality and performance, particularly as they relate to Jordan's education and healthcare systems. MoDEE has also studied the network potential to support the business sector in Jordan and increase access in under-served areas to support the growth of traffic demand as the pace of technology diffusion accelerates (MoDEE 2020c). The GoJ is currently opening the NBN to private sector participation.

Jordan has the potential to create a favorable environment for developing an advanced digital infrastructure. There is potential for private sector contributions (e.g., broadband networks and data infrastructure). This potential for success is amplified by MoDEE's strong technical and policy competence in the sector, and the country's independent regulator, i.e., Telecommunication Regulatory Commission, (TRC) that maintains an open and liberalized telecommunications market in the country.[4]

TRC has recently taken agile measures to maintain service quality during the COVID-19 pandemic. An emergency committee was formed with senior chief technology officers (CTOs) of network operators to enhance the resilience of the networks and ensure continuity of services. As a result of its decision to allow providers to temporarily utilize additional spectrum, the measures led to an increase in the average download speeds for mobile users by 54% during the period March – May 2020. The additional spectrum allowed operators to cope with the additional 8% in data traffic and stresses on their networks during the country's lockdowns (Barton 2020).

Cloud Infrastructure

Jordan is aiming to enhance its cloud infrastructure and increase its data storage capacity. Recently (in July 2020), a national cloud computing policy has been adopted. The policy has benefited from several stakeholders' inputs as MODEE conducted public consultations starting in January 2020. A hybrid approach was adopted in this Cloud policy for establishing a National Government Cloud (private cloud) to be managed by MoDEE, while encouraging the expansion of Commercial Cloud (global and local public cloud) open to licensed service providers through TRC[5]. The enabling policy is progressive and takes into consideration the rapid changes in technologies, with clear reference to the need for adaptability given the potential rise of emerging technologies such as Quantum computing, Fog and Edge computing, and the Internet of Things (IOT). However, the policy is also unclear in a few areas, like the privacy provisions that cloud providers may face when enforcement authorities made requests for data (stored locally and/or overseas) (MoDEE 2020b).

The government's data infrastructure is mainly built on a Government Private Cloud (GPC). It is part of the Secure Government Network (SGN) linking over 100 government entities. The National Information Technology Center (NITC), now part of the MoDEE, hosts a consolidated data center to run the GPC. The cloud stack[6] provides scalable virtual machines, virtual networking and databases. MoDEE offers a set of cloud services to government entities, including software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). Further cloud services to government entities also include database-as-a-service, email-as-a-service, rapid software development-as-a-service and others. However, MoDEE's currently operated and managed data center has relatively limited capacity, and there are on-going efforts to advance the development of a national government cloud and a certified recovery center.

A comprehensive cybersecurity policy framework was adopted in 2019 to protect the security of the government's data infrastructure. The security areas include physical security, information security and assurance as well as business continuity[7]. The government also established the National Computer Emergency Response Team (JO-CERT), under the NITC, to prevent, respond to and recover from cyber incidents and attacks. JO-CERT was recently re-organized as a separate department under the e-Government administration of MoDEE, after the merging of the NITC into MoDEE and its restructuring in 2019. All information assets under the management of MoDEE and NITC, including data centers, are subject to the ISO 27001 security standard and the ISO 31000 risk management standards. The data center is

[4] The Ministry of Finance (MoF) has also a clear vision of PPPs in the country, led by a specialized PPP Unit.

[5] The TRC's regulatory regime spans both the telecom and IT sectors. TRC's main role in this context is to monitor and ensure the quality of services offered by cloud service providers and prepare license agreements with them.

[6] The stack is based on Microsoft Windows Azure Pack (WAP)

[7] Interview with Ms. Nada Khater, MoDEE. March 1st, 2020. Amman, Jordan.

following the Tier 3 standard, with 4 access layers of security and separated to different security zones (Internet, DMZ and Backbone) by a dual firewall architecture.

There is a robust potential for scaling cloud infrastructure that has yet to be materialized in Jordan. According to TRC, the three main telecom operators (i.e., Zain, Umniah and Orange) as well as a few private providers are currently offering commercial cloud services in Jordan, including commercial uses, internet of things (IOT) and data retention. Additional cloud hosting capacities are also available in Jordanian enterprises such as the Jordanian Electric Power Company (JEPCo). Several small-capacity datacenters have also been established as part of the National Broadband Network (NBN) at 85 sites including schools and substations (shelters) across the Kingdom.

Data Interoperability Framework

Data interoperability is essential to access and process data from multiple sources. This is done without losing meaning, and then linking or integrating the data for mapping, visualization and other forms of representation and analysis. Interoperability enables people to find, explore and understand the structure and content of datasets. Data interoperability enables data from different sources to be combined help create more holistic and contextual information for simpler (and sometimes automated) analysis, better decision making and accountability purposes.

At this stage, MoDEE supervises the linkage between different datasets in public entities through a Government Service Bus (GSB). Currently, transfer of data between public entities is possible using standard web services, APIs through the GSB and a middleware infrastructure[8] that enables Service Oriented Architecture (SOA) by acting as an intermediary layer in which a set of reusable government services are made widely available. The GSB is built on the Secure Government Network (SGN), itself built on the National Broadband Network (NBN). The main role of the SGN is to provide connectivity to government entities in a secure manner. In addition to the GSB, other services are provided through the SGN, including file-sharing/exchange, e-mail, inter-application communication, and the Government Private Cloud (GPC).

Adopting and adhering to data standards are also vital to foster interoperability and integration. The country is still with a relatively incomplete standards ecosystem[9], but some progress on foundational elements is taking place such as in the area of data classification. Data classification optimizes the use of data centers and cloud infrastructure but is also relevant to other initiatives such as an established Open Data approach. Data classification is thus necessary to determine how data should be stored and made available on governmental or commercial clouds.

A new Government Data Classification and Management policy was recently approved in Jordan. Developed by MoDEE in 2019 (MoDEE 2019), the policy was approved by the Council of Ministers in January 2020. This framework for data management includes the adoption of a data governance model for each public entity, the creation of data inventories, data classification and publishing. The directives require over 120 governmental entities to classify the datasets under their control within 12 months. This has the potential for establishing a uniform data classification and management system.

The current data classification scheme is based on four levels (Secret, Sensitive, Private and Public). Both secret and sensitive data should be hosted inside the government and inside Jordan. While Private data remains inside Jordan, normal data (for public use) could be hosted outside Jordan, including commercial cloud providers. The table below provides a reference to the impact level of a security breach associated with each of the above four Data Classification categories, and a few indicative examples of the type of information that could be brought under each of these categories. These classification levels approved in the regulations are also equivalent to the ones referred to by the Access to Information Law.[10]

[8] The middleware is built with IBM DataPower Gateway.

[9] A data standards ecosystem includes the full range of data standards, classifications, foundational models, and vocabularies or ontologies.

[10] Law No. 47 of 2007. Guaranteeing the Right to Obtain Information. Published in the Official Gazette No. 4831, p. 4142, 17 June 2007.

Table 2.1. Impact level and examples of information for each Data Classification category

Data classification categories	Impact of possible Data Security breach	Examples of data or other information falling under the relevant category
Secret (highest level of security)	Security breaches relating to such Data can be expected to have a severe or catastrophic effect on the State's operations or assets, public security or the lives of citizens.	Information relating to confidential exchanges with other countries, national defense or national security
Sensitive (high medium level of security)	Security breaches relating to such Data are very likely to cause serious damage to State or public legitimate interests, and possibly also to individuals.	Formal or informal information between different government authorities in the preparation of an official government document or policy; information relating to public criminal investigations, or involving business or industrial property that may not be publicly disclosed
Confidential and shared (medium level of security)	Disclosure of such Data outside the Government authorities authorized to share or other security breaches may cause limited harm to the State or the public, and potentially more important harm to individuals whose Data are affected by such breach.	Information which, while sensitive (e.g., because it relates to sensitive personal data) is exchanged and needs to be shared between certain Government authorities in the framework of their duties (e.g., minutes of meetings, information on citizens, inventories, etc.)
Public	Disclosure of such data to the public will have no negative impact and may actually add value to the Data. Nevertheless, it is still important to ensure the Data Set's integrity and continuing public availability after its release to the public.	Information on government authorities' structures, tasks, list of persons responsible for specific tasks; budgets, policies, work plans, reports, studies, statistics, procedures, agreements with private or public parties, procurement procedures and policies, etc.

Source: MoDEE 2019.

Open Government Data

Jordan has made progress on Open Government Data in the last two years. An Open Data Policy, prepared in July 2017 and subsequently approved by the Council of Ministers, represents the foundation for such progress. MoDEE has developed a framework for open government data that includes creating an open data portal, training entities to classify and prepare data for publication. All data in the custody of the Government of Jordan, regardless of form are managed under the Data Classification Management policy (MoDEE 2019) including the explanation of how government data should be stored, managed and published. The policy introduced for the first time a new role of a "Data Coordinator" within each public body, responsible for data classification and selecting which datasets to open, assigning a "Focal Point" responsible for uploading datasets to the government portal[11]. An Open Government Data License was also applied to allow government entities to publish data without copyright restriction.

MoDEE is currently working on a Data Quality Framework for Open Data. Open datasets published by the Government are open to all and licensed under a Jordanian Open Government Data License, which allows use, reuse and sharing of data, in compatibility with the Creative Commons (CC-BY) license. Under the license, any person can use, copy, publish, distribute, transmit or process the data and make it available to third parties. They can also develop new derivatives of the data by combining them with other data or using them in a product or service. When used, the data should be attributed to the publisher(s) using a specific statement. Also, the current Open Government Data portal allows the retrieval of datasets by downloading files within a limited set of open formats, which limits their re-use and

[11] https://data.jordan.gov.jo

integration with other systems. To overcome these technical barriers, MoDEE is planning to provide a set of publicly available APIs in a potential new data portal.

Implementation of the Fourth Action Plan (2018-2020) of the Open Government Partnership (OGP) is also a priority in Jordan (MoPIC 2018). The emphasis is on building the institutional capacities and ensuring the participation of various stakeholders regarding open data. In cooperation with ESCWA and the Ministry of Planning and International Cooperation (MoPIC), MoDEE organized a workshop in 2019 for representatives from various ministries and nongovernmental organizations, to address the technical aspects of open data and advance the participation agenda in Jordan's national context (UN ESCWA 2019).

Box 2.1: Ten Principles for Opening Up Government Data

The Sunlight Foundation is a US-Based nonprofit organization that promotes open government, accountable and transparent to all. It has developed "Ten Principles for Opening Up Government Information" that are broadly considered by experts to discuss how government could open government data for public use. The principles are listed as follows:

- **Completeness:** the datasets should be as complete as possible, reflecting the entirety of what is recorded about a subject. All raw information, datasets, and Metadata should be released to the public.
- **Primacy:** government entities are the primary source of data, with the ability to provide details on how the data was collected and prepared to be published.
- **Timeliness:** the data should be available to the public as quickly as it is gathered and collected.
- **Accessibility:** the datasets should be as accessible as possible, with accessibility defined as the ease with which information can be obtained, whether through physical or electronic means for all end users.
- **Machine** readability: the datasets should be machine-readable, that can be downloaded, processed, and used by any open programs or technology, data should be stored in file formats that can be electronically processed.
- **Non-discriminatory:** any person can access the data at any time without having to identify him/herself or provide any justification for doing so, such as pre-registration requirements or not to allow access to data but through specific applications.
- **Non-Proprietary:** the data must be prepared for publication using an open format, data access does not require specific software or programs that require licenses to be used, and that is, it can be used without any fees or costs.
- **Licensing:** data is not subject to any copyright, patent, trademark, or trade secret regulation. Reasonable privacy, security, and privilege restrictions may be allowed.
- **Permanence:** data should remain online, with appropriate version-tracking and archiving over time.
- **Usage costs:** the cost of identifying, exporting, conforming to the standards, and downloading the required datasets should be considered.

Source: Sunlight Foundation 2017

The implementation of open data government is not without challenges. In practice, civil servants are applying the data classification policy conservatively as a risk mitigation mechanism, resulting in data being classified unnecessarily as "sensitive" or "secret." This creates demand (user side) issues that reduce data usage and contribute to eroding citizen trust. This situation is amplified by the former classification of government information that fell under the Protection of State Secrets and Documents Law[12] which made secrecy of information the general rule and disclosing information the exception. A shift in culture to proactive disclosure within the public administration is necessary to overcome such habits. As of March 2020, nearly 230 datasets were published by 35 governmental entities. Nevertheless, the use and re-use of published government data remain limited.

To date, the adopted instructions determine a set of metadata to be published with each dataset. Still, they do not point to specific standards to be adopted in this regard. Public entities should also perform data anonymization techniques before publishing datasets that might contain personal data. As no legal definition of "personal data" is found in Jordanian law, these techniques are defined in the instructions as "any data process that ensures the inability to identify a natural person."

Access to Information

Jordan was the first country in the Arab States to pass an Access to Information (ATI) law in 2007.[13] The ATI Law grants Jordanians the right to request access to government records only if they have a "lawful interest or justification." Despite the existence of such a right, the ATI law's enforcement and implementation have its limitations.

No information bearing on the nature of religious, racial, ethnic or sexual discrimination can be requested. There are also several exceptions that challenge the disclosure of a broad set of information, including secrets related to national defense, state security or foreign policy, personal information related to education or medical records, professional records, bank accounts and transfers and professional confidentialities, and, correspondences having a personal or confidential nature. The law also forbids the disclosure of any information that will lead to the violation of copyright, intellectual property, or fair or lawful competition or to illegal profit or loss for any person. Investigations made by the prosecution, judicial system or security authorities concerning any crime or lawsuit cannot be disclosed. Finally, there is a significant administrative burden associated with submitting requests, uneven application procedures and compliance across the public administration.

The Information Council is responsible for the implementation and promotion of access to information in Jordan. An annual report about the ATI law's implementation is prepared and submitted to the Prime Minister and Cabinet head. In 2018, government entities received 6,490 requests to access information, a decline from 13,004 in the previous year; 39 requests were rejected[14]. The reasons for rejection have not been disclosed as these reports are not made public.

Jordan's latest Open Government Partnership Action Plan (2018-2020) includes a commitment to strengthen the enforcement of the ATI law through a participatory process. A new draft law has been referred to the legal committee of the Lower House in January 2020 for consideration. One of the proposed amendments is the restructuring of the Information Council to be equally composed of government entities and representatives from civil society (i.e., 50-50 split). A new institutional protocol drafted by the Department of the National Library (DNL), MoDEE and civil society organizations to effectively enforce access to information is expected to introduce the proactive disclosure of data, allowing public bodies to publish open data without obtaining access to information requests. These changes were suggested based on previous recommendations from media and civil society organizations.

The Jordanian public sector plays a significant role in data collection and management. While there are no formal government policies on data stewardship, ownership and licensing, large amounts of data are being collected and then stored by governmental agencies that have the power to regulate how others might access it. Generally, there are no distinct or clear roles within public agencies to determine whether the stored data is considered a potential asset that can provide economic benefits, and which data have service potential. This role is played primarily by MoDEE within its

[12] Protection of State Secrets & Documents Provisional Law No. 50 for the year 1971. For further analysis of the law, see Article 19 (2005).

[13] Law No. 47 of 2007.

[14] Interviews with the National Center for Human Rights (NCHR) and Jordan Open Source Association (https://jordanopensource.org/) in March 2020.

e-government directorate, that cooperates with different entities to prioritize services to be developed and made accessible on the e-government platforms.

Safeguards: Fostering Trust in Data Processing and Use

Building trust in the collection, sharing, utilization, and governance of data is essential for realizing the full potential of these data. While some safeguards to protect the security of data under the Cybersecurity policy strategy and law, Jordan does not yet have a specific legal framework to protect the personal data or personally identifiable information of individual data subjects. This is a key element in fostering trust in data processing and use, and a pre-requisite in enabling cross-border trade in data with jurisdictions that have adopted adequacy requirements before transferring data, such as the European Union.

Jordan's strategy towards data governance is described as a "hybrid" approach, designed to take advantage of opportunities arising from the use of data, while protecting individuals' rights in their personal data, as well as the integrity and security of public sector data.

Personal Data Protection

Jordan has not yet adopted a Personal Data Protection Law. The Jordanian Constitution, promulgated in 1952, recognizes the right to privacy: Article 7 guarantees personal freedom, and that infringements on the rights and public freedoms or the inviolability of the private life of Jordanians is a crime punishable by law. Separately, Article 18 establishes that "All postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law."[15] Jordan is also a signatory to relevant international instruments, such as the International Covenant on Civil and Political Rights (ICCPR)[16], ratified in 1975, and the Convention on the Rights of the Child in 1990. Additionally, Jordan signed the Cairo Declaration on Human Rights in Islam in 1990. Together, these frameworks provide a robust legal foundation for Jordan to enshrine a rights-based approach to data protection in its upcoming data protection law.

Jordan began its process of drafting its personal data protection law in 2012. In 2014, the Jordanian Ministry of Information and Communications Technology (now the Ministry of Digital Economy and Entrepreneurship, or MoDEE) proposed a draft law. A public consultation on the law was launched in 2016, led by a multi-stakeholder committee composed of the Ministry of Interior, Ministry of Labor, Ministry of ICT, the Telecommunications Regulatory Commission, the Central Bank of Jordan, and the Information and Communications Association of Jordan (INTAJ), the leading industry association. The most recent draft developed by MoDEE is currently being reviewed by the Legislation and Opinion Bureau (LOB), in advance of being proposed to the Parliament.

Overall, the latest draft data protection law[17], which was designed to be modeled on the EU General Data Protection Regulation (GDPR), is aligned with good practice laws on data protection. It provides limitations on the collection and use of personal data, as well as obligations on data processors and controllers. It also provides for several rights to data subjects that are in line with those protected under international principles or guidelines on privacy and data protection elaborated by the OECD (2013) and the UN (2018), as well as in legal instruments such as GDPR. The inclusion of certain rights such as data portability is advanced relative to other countries in the region, and a key enabler for better data use. That said, the draft law includes certain provisions that are either unusual or depart from international good practice in several dimensions and could benefit from clarifications or amendments as it is finalized by MoDEE and the Legislative Oversight Bureau.

Important good practice provisions remain missing from currently available drafts under discussion, including specifying additional protections to be required for sensitive data, broadening the scope of categories to include biometric data, and clarifying lawful bases for data processing other than with consent (such as requiring data collection and processing activities to be subject to a legitimate purposes test and necessity and proportionality requirements).

[15] An English version of the Constitution is available at: http://cco.gov.jo/Portals/0/constitution_en.pdf

[16] See article 17 on the protection of private life.

[17] Unofficial draft of the law shared by MoDEE and reviewed by the World Bank. The law is currently being reviewed by the Legislative Oversight Bureau.

The explicit clarification of lawful bases other than consent is particularly important to ensure that data transactions for which it would be difficult or highly costly to obtain informed consent, such as data processing by public authorities[18] and "passive" forms of data processing (e.g. use of biometric data for authentication or verification or processing credit data for financial oversight) are subject to reasonable limits on use that protect the rights of data subjects.

Additionally, the law would benefit from the inclusion of other safeguards that promote accountability, such as the requirement to minimize the amount of data collected ("data minimization"), limitations on automated decision-making (beyond profiling), and the requirements to incorporate technical and organizational privacy by design and default principles or use privacy enhancing technologies to protect data. Additionally, the law would be strengthened by requiring data controlling entities to undertake Data Protection Impact Assessments to identify and manage risks associated with certain types of data collection and use. Given the drafting intention to keep the law high-level, provisions that are considered too detailed to be included in the law of general application should be elaborated on in future implementing regulations.

The draft law includes an exemption clause for SMEs. While the intention behind the inclusion of this clause is reasonable, given criticisms leveraged against legislative or regulatory frameworks, such as GDPR, that adopt "symmetric" liabilities[19] which disproportionately affect smaller organizations in terms of compliance burden and broader competition dynamics. That said, there is a question as to whether this exemption clause could be exploited by businesses seeking to avoid compliance. Further clarity on enforcement will need to be provided in the implementing regulations and reviewed by the Personal Data Protection Council (the Data Protection Authority, or DPA).

The Personal Data Protection Draft Law limits cross-border data transfers to third parties on data protection grounds. The draft introduces a set of conditions under which personal data can be transferred to non-domestic third parties: they should have an equivalent level of protection, and the original data controller should ensure the level of protection is adequate before the transfer of data. Additionally, the Personal Data Protection Board is responsible for issuing a regularly updated list of countries or entities that are deemed to have enough levels of protection in accordance with the provisions of this law. This is consistent with the adequacy approach proposed under GDPR. That said, the GoJ may consider adding provisions on conditions that would be considered when determining an adequacy arrangement (e.g. international obligations/covenants that the 3rd country is a party to, rule of law, human rights norms and standards[20]) to support the transparency and predictability of the adequacy process. In addition, the GoJ may consider including provisions to regularly review adequacy decisions, particularly if circumstances change. Should adequacy levels change, the law should require data controllers to take compensatory measures to protect personal data, including using Binding Corporate Rules or Standard Contractual Clauses. Recent litigation in the European Court of Justice[21] have highlighted the importance of creating legal frameworks that take a holistic approach to accountability, rather than viewing compliance as a mere "tick the box" exercise, and the robustness and predictability of the legal regime for cross-border transfers will be essential to enable Jordan to participate effectively as a regional or global player in the data-driven economy, particularly in terms of engaging in digital trade with the EU.

The institutional arrangements designed in the data protection draft legislation to support the enforcement of the rights and obligations are unusual and risk affecting the independence and effectiveness of the data protection authority. Rather than establishing an independent entity, the personal data protection draft law provides for the creation of a multi-stakeholder Data Privacy Board appointed by the GoJ, located within MoDEE, composed of members from the GoJ, the security apparatus, Parliament, and independent experts, including from the private sector and civil society.

[18] As good practice data protection legislation such as GDPR highlight (see recital 43), the power asymmetry between public sector entities and end users makes a "legitimate interest" standard as a lawful basis for processing more appropriate than consent for data processing by public authorities, given the difficulty of seeking "informed consent."

[19] GDPR imposes fixed fines on data controllers, either up to EUR20 million, or 4% of turnover for particularly severe fines. article 83(5) of GDPR.

[20] According to Article 45 of GDPR, relevant criteria may include whether the third party respects the rule of law; human rights/fundamental freedoms; relevant legislation (including concerning public security, defense, national security, criminal law, etc.), data protection rules, including for third party transfers of data, has mechanisms that enable the effective administration of judicial redress; the independence and adequate enforcement of national supervisory authorities; international commitments the third country or organization is a party to.

[21] See the CJEU's judgment in Schrems II (2020), in which it invalidated the Privacy Shield, the adequacy mechanism regulating cross-border data transfers between the EU and the US. The decision by the Irish Data Protection Commissioner (DPC) issued in September 2020 further invalidated the Standard Contractual Clauses (SCCs) relied on by Facebook to legally transfer data from the EU to the United States (Lomas 2020).

While inclusion of civil society and other external stakeholders does not per se preclude independence[22], the structure and composition of the Board, particularly the inclusion of security forces and private sector representatives, risks creating conflicts of interests or impeding its independence, particularly about its roles in investigating data breaches and issuing fines. The lack of clarity around staffing criteria (including specifications of the skills required for technical roles) and resource allocation in the law or secondary legislation may further affect the Board's effectiveness. This is particularly concerning given the current absence of an independent right to redress through the courts in the law of general application. Together, these limitations may have a negative effect on data subjects' trust in the institutional arrangements, with implications on their willingness to engage in the data-driven economy.

In addition to supporting the strengthening of the data protection authority, the GoJ could promote accountability in data processing and decentralize the oversight process by requiring entities that collect and process personal data to appoint a Data Protection Officer, who would be an intermediary between the entity and the data protection authority. The inclusion of clear guidelines on appointment and criteria for data processing to be reviewed by the DPO should be clarified to support the effective enforcement of this role and improve the predictability of the legal framework on data protection.

Beyond the draft Personal Data Protection Law, certain sectoral laws include provisions that are related to data protection. For example, in the Telecommunication sector, that is regulated through the Telecommunications Regulatory Commission (TRC), the Telecommunications Law No. 13 of 1995 includes provisions to protect the beneficiaries of telecommunications services. The regulatory regime of the TRC spans both the Telecommunications and IT sectors, including the cloud services available to the public for commercial uses and certificate providers. The TRC also issued instructions to regulate the retention of telecommunications records and to ensure the protection, safety, security, and privacy of data. The Telecommunications Law criminalizes unauthorized interception of private communications and defines the penalties for impeding communications in any way.

Consumer Protection

Consumer Protection laws and regulations can promote trust in the digital economy by protecting against unfair or deceptive commercial practices. In some cases, they can also be leveraged as complementary protections to data protection legislation to protect the personal data rights of individual consumers in an electronic commercial transaction. While consumer protection legislation has long existed and is well established in many jurisdictions, only around 50% of countries globally have specific legal protections for online consumers.[23]

Jordan features among this group of countries that have not adopted a specific legal framework for online consumer protection. The Consumer Protection Law No. 7 of 2017 defines broad consumer rights, such as the availability of goods and services without damage, access to "complete and correct information" displayed on goods or services before completion of supply process", "selection without undue pressure", as well as prosecution of infringements and compensation (UNCTAD 2017). The law is designed to be horizontally applicable, rather than establishing sector-specific rules. The right to invoke additional rights through sector-specific regulation is enshrined as a right under the 2017 law.[24] While the right to form or join consumer protection associations is not enshrined in the Consumer Protection law, such associations play an important intermediation role in supporting consumer rights in Jordan (UNCTAD 2017).

While the absence of explicit reference to e-commerce in the Jordanian Consumer protection Law does not necessarily preclude it from extending to such transactions, ensuring that the scope of the Law explicitly covers e-commerce can enable it to be fit for the digital age and to be leveraged as a more effective safeguard by consumers. Good practice guidelines on consumer protection, including the OECD Guidelines for Consumer Protection in the context of Electronic Commerce (2000) and the UN Guidelines on Consumer Protection (UNCTAD 2016) include

[22] For example, the Belgian Data Protection Authority has been confronting the question of the independence of its external members of its "Knowledge Center" since 2019. See POLITICO, "Belgian data regulator roiled by infighting", November 19, 2020, available at: https://www.politico.eu/article/belgian-data-regulator-accused-of-violating-eu-rules/; the Belgian Commercial Court was meant to rule on this issue on February 24, 2021, but delayed its decision.

[23] According to UNCTAD's Cyberlaw tracker, 56% of countries have legislation for online consumer protection; 6% have draft legislation; 9% have no legislation. A key constraint is the lack of data in this area, with nearly 30% of countries not having published data on the existence of legal protection for online consumers. Of the countries who have a specific legislative framework, the adoption varies significantly by region: 73% in Europe, 72% in North and Latin America, compared to 46% in Africa. See https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx

[24] Article 24 of the 2017 Consumer Protection Law. See also UNTAD (2017).

expanded provisions to protect online consumers and improve transparency and accountability in e-transactions given the specific legal challenges that arise in these markets. Options include ensuring that existing consumer protection laws or implementing regulations and technical guidance for enforcement authorities make it clear the law covers both online and offline transactions, or adopting laws specific to e-commerce platforms[25], which may provide countries with the opportunity to better tailor regulation to these types of transactions (Molinuevo and Daza Jaller 2020).

In terms of institutional arrangements, the 2017 Law provides for the creation of a Consumer Protection Council, under the leadership of the Minister of Trade, Industry and Supply. The multi-stakeholder membership includes the heads of key sectoral entities, the Jordan Chambers of Commerce and Industry, and representatives of non-governmental stakeholders, including of consumer protection associations, higher education institutions, the federation of farmers, and private sector organizations. The mandate of the Council includes receiving and investigating complaints and coordinating with relevant sectoral authorities.[26] Membership terms are for two terms, renewable once.

Cybersecurity and Cybercrime

The policy and legal framework for cybersecurity (including the security of data infrastructure) are defined by the National Cybersecurity Strategy 2018-2023, the 2015 Electronic Crimes law and the 2019 Cybersecurity Law.[27] The National Cyber Security Strategy 2018—2023 aims to build upon the objectives of the 2012 strategy and National Cybersecurity Programme (NCP) to enhance trust in and resilience of the Critical National Infrastructure, government, businesses and the public against existing and emerging cyber threats. These include leaks of classified or sensitive government data, particularly relating to defense, security or critical industries, as well as the misuse of data subject to intellectual property rights.[28] The strategy lists specific security challenges, including terrorism and political or ideological disruption, which the GoJ considers to be emerging as key motivations for cyberattacks, beyond financial or economic incentives. Other security challenges relate to emerging technologies or uses, including Internet of Things (IoT) and cloud computing, especially regarding how security and privacy concerns are managed by cloud providers. A key organizational challenge (and focus area[29]) highlighted in the current strategy is the critical skills shortage of cybersecurity professionals in both the public and private sectors.

Jordan adopted a Cybercrime Law (Electronic Crimes) in 2015[30], replacing the 2010 "internet regulation law", that criminalizes unauthorized access to systems or other databases. The Law defines a set of penalties for all who intentionally access a website or information system or intercept or copy users' data from a website without authorization or in excess or violation thereof. Additionally, the law criminalizes the unauthorized input, alternation, deletion or interference with a computer system or platform[31] as well as the fraudulent use or alteration of data or system.[32] The law specifies specific penalties for fraudulently obtaining financial data, including credit cards or data used in the execution of electronic financial or banking transactions. The scope of the law also extends to broader criminalized activities, including the sexual exploitation of minors or individuals with mental or psychological disabilities through the transmission, publishing, promotion or use of pornographic material[33], or promoting prostitution.[34] In addition, the cybercrime law covers acts such as supporting terrorist activities.[35] Other provisions, such as criminalizing the intentional sending, resending, or publishing data or information through the web or electronic websites or any information system of defamatory, libelous or slanderous content, even if such actions are not directly linked to a crime,[36] or accessing classified data or information that touches upon national security, foreign relations of Jordan, general security or national

[25] This is the approach adopted by China, which imposes extensive responsibilities on e-commerce platforms, including holding them liable for failing to provide information on vendors who breach provisions. Conversely, the United States and the European Union place the onus more on users (Molinuevo and Daza Jaller 2020).

[26] Article 9 of the 2017 Consumer Protection Law. See also UNCTAD publication (ibid.)

[27] Law no. 16 of 2019

[28] See section on "the evolving threat landscape" in the 2018-2023 strategy

[29] The Strategy includes a focus on developing a Security Awareness and Capacity Building Program, in consultation with academia and international partners to ensure adequate human resource and technical capacity domestically to respond to local and foreign cyberthreats.

[30] The Electronic Crime Law No. 27 of 2015

[31] See article 5: "Intentionally capturing, interfering with, or intercepting what is transmitted through an information network or any information system"

[32] See article 4: "Entering, publishing, or intentionally using a program through the web or any information system to delete, add, damage, release, block, move, copy, or capture, or enable others to view data or hinder or impersonate the owner of the article without an authorization shall be penalized."

[33] Article 8 of the 2015 law

[34] Article 9 of the 2015 law

[35] Article 10 of the 2015 law

[36] Article 11 of the 2015 law

economy[37] go beyond the usual scope of cybercrime legislation and have been criticized by civil society organizations for being overly broad (see below).

The scope of the law does not preclude the applicability of sectoral regulations. For example, the confidentiality of financial data is also handled by a handful of other laws and regulations, including the Banking Law No. 28 of 2000 and the instructions issued in 2017 by the Central Bank of Jordan (CBJ) on the Protection of the Personal Data of the Clients of Payment Services and Electronic Transfers. Proposed amendments to the 2015 Law in 2017, proposing to criminalize online hate speech with severe penalties (a term of up to three years and a maximum fine of 10,000 JAD (around $14,000) for "incitement") and broaden the scope of the law to cover "applications" in addition to existing information systems[38], were severely opposed by civil society. The main criticisms included the unclear definition of "hate speech" and the perception that these provisions infringed on freedom of expression and may be instrumentalized to crackdown on civil society expressing legitimate criticism of public officials on social media (Access Now 2019). Following public pressure, the GoJ withdrew the draft law at the end of 2018. Since then, amendments to the law were discussed in Parliament in February 2019 (Access Now 2019), but its current status is unclear.

The 2019 Cybersecurity law[39] provides for the establishment of the National Cybersecurity Council (the oversight and coordinating layer) and the National Cybersecurity Center (NCC), responsible for the operational or technical aspects of cybersecurity. The Council will be composed of members from the Ministry of Digital Economy and Entrepreneurship (MoDEE), the Jordanian Armed Forces, the Central Bank of Jordan, the General Intelligence Department, the Public Security Directorate, and the National Center for Security and Crisis Management. The council's chairman is appointed by royal decree.[40] The composition of the council demonstrates an awareness among Jordanian officials that interagency coordination is necessary to develop and implement an effective cybersecurity policy (MEI 2020). This is a change from the previous centralized approach, in which the Ministry of ICT (now MoDEE) led the development of cybersecurity policy. The National Cybersecurity Council (NCC) is responsible for approving strategies, policies and standards related to cybersecurity; approving plans and programs needed for the NCC to perform its duties, including with regard to international and regional cooperation; approving quarterly reports on Jordan's performance in cybersecurity; forming coordinating committees to support implementation and approving the annual budget of the NCC[41]. At the time this report is being prepared, it is unclear if the NCC is operational.

The NCC leads the strategic orientation and operationalization of the country's cybersecurity policy under oversight of the Prime Minister's Office.[42] The NCC's mandate includes determining Jordan's Critical National Infrastructure and setting the requirements for its protection, including Information Security, from cyberattacks. To support this, the NCC is responsible for preparing strategies, policies and standards for cybersecurity, and develop and execute cybersecurity operations to support CERTs in the public and private sectors to respond to threats. The NCC's mandate also includes providing licenses to the providers of cybersecurity services. Its duties include monitoring, evaluating and reporting on the status of cyber-preparedness and security to the Council, including by establishing a database of threats, evaluating cyber security incidents resilience teams, and preparing annual reports.[43] It is also responsible for coordinating and collaborating with domestic and international organizations to mitigate cyber risks and promote research on good practices. The NCC is responsible for receiving and reporting complaints on cybersecurity incidents and responding or escalating them accordingly.[44] Article 16 of the 2019 Cybersecurity Law provides the NCC with the authority to respond to breaches in a manner proportionate to the threat, from providing written warnings to blocking, shutting down or suspending the telecommunications network, information system, devices or private electronic messages of the relevant parties. Other measures can include cancelling or suspending licenses of cybersecurity service providers or imposing fines.

[37] Article 12 of the 2015 law

[38] See Articles 11 and 13 of the draft Cybercrime Law. See also MEI (2020).

[39] The law defines cybersecurity as the procedures taken to protect IT systems, networks and critical infrastructure against cybersecurity incidents. It defines "critical infrastructure" as the set of systems, e-networks, tangible and intangible assets, cyber assets and systems whose continuous operation is considered a necessity to guarantee the security of the state, economy and society.

[40] Article 3 of the 2019 Cybersecurity Law

[41] Article 4 of the 2019 Cybersecurity Law

[42] Article 5 of the 2019 Cybersecurity Law

[43] Article 6 of the 2019 Cybersecurity Law

[44] Article 8 of the 2019 Cybersecurity Law

The conditions of retaliatory measures are determined in accordance with the Council.[45] In terms of implementation, existing Governmental and defense and security computer response teams are the Jo-CERT and JAF-CERT respectively.

E-Transactions

E-commerce or e-transactions laws are a key enabler for domestic and cross-border transactions for use in the public sector (Government e-services) and for the growth of data-driven products and services in the digital economy. Jordan was one of the first countries in the region to adopt an Electronic Transactions Law in 2001.[46] In 2015, this law was repealed and replaced with Law No. 15 of 2015 concerning Electronic Transactions.[47] The 2015 Law was designed to support the growth of e-commerce by providing a legal framework for conducting business transactions online and making contracts via electronic means of communications.[48] The law allows government and public administration to conduct all pertinent transactions and communications electronically by granting legal equivalence between paper based and electronic transactions.[49] In this regard, the e-transactions law is aligned with international good practice on the regulation of electronic communications, chiefly the UNCITRAL Model Law on Electronic Commerce (1998), which promotes functional equivalence in the treatment of electronic documentation. It also allows for the online payment of fees.

The GoJ has adopted a hybrid approach to legal recognition of e-signatures: the legal framework recognizes the legal validity of electronic signatures[50], regardless of the method of signing chosen by the parties; however, qualified signatures (such as digital signatures paired with a certificate issued by a licensed certification service provider or authority) are given evidentiary presumptions, including of validity and authenticity (Molinuevo and Daza Jaller 2020). The Law gives legal recognition to all electronic signatures to secure and authenticated electronic transactions, [51] and distinguishes between three types: (i) ordinary, (ii) protected[52], and (iii) authenticated[53] electronic signatures, that differ by their level of security and accreditation of the issuing entity. However, different levels in qualification of e-signatures have implications for their evidentiary weight: parties seeking to rely on ordinary e-signatures to prove the validity of an electronic contract will need to prove the signature's validity; protected e-signatures can be relied on as evidence for the validity of the transaction by both parties. Authenticated e-signatures carry the same validity as protected signatures but can be relied upon as evidence by third parties as well.

Hybrid, or two-tiered, approaches to the legal recognition of e-signatures as it provides parties to a transaction with the flexibility to select the more appropriate method and technology of signing for the specified transaction, while recognizing that certain types of transactions may require specific procedures and technologies to authenticate and guarantee the integrity of the electronic communication (for example, to submit certain documents to the government) (Molinuevo and Daza Jaller 2020). More prescriptive approaches, which consider only the digital signature to be valid, can create unnecessary bottlenecks and costs for parties, and can be a significant impediment to the scalability of G2C/C2G and particularly B2B e-transactions.

[45] Article 16 of the 2019 Cybersecurity Law

[46] Law No. 85 of 2001 concerning Electronic Transactions

[47] Law No. 15 of 2015 concerning Electronic Transactions, adopted on 17 May 2015. Available at: https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=103025&p_lang=en

[48] See UNCTAD Global Cyberlaw Tracker. https://unctad.org/topic/ecommerce-and-digital-economy for note 2. For an English translation of Jordan's Law No. 15 of 2015 concerning electronic transactions, see the ILO's NATLEX database. http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=103025&p_count=96946

[49] E-transactions are defined as "transactions carried out by electronic means". See articles 7,8 of the E-transactions Law No. 15 of 2015

[50] The UNCITRAL Model Law on Electronic Signatures of 2001 lays out the conditions for the legal recognition of e-signatures and the responsibilities and liabilities of the contracting parties. E-signatures must be considered legally valid, and their authenticity (i.e. able to prove that it belongs to the signatory) and integrity (that the signature and the underlying information) must be proven.

[51] E-signatures are defined as "data in the form of letters, numbers, codes, or symbols and which is electronically, or in any other similar mean, included in, affixed to, or associated with an electronic record and is used to authenticate the identity of the signatory and differentiate such individual from others". See Article 10

[52] Electronic signatures are deemed protected if all of the following conditions are met: (i) if it is unique and distinguishes the signatory from others; (ii) if it identifies the signatory; (iii) if the private key is under the control of the signatory upon signing; and (iv) if it cannot be subsequently modified on the electronic document after signing. See Eversheds and Sutherland (2020).

[53] In addition to the conditions for protected signatures, e-signatures are deemed "authenticated" if they are certified by one of the following institutions: (i) an electronic authentication party licensed in Jordan; (ii) an accredited electronic authentication party; (iii) any governmental body legally authorized by the Council of Ministers, including ministries, public institutions or municipalities provided that they fulfil the requirements of the TRC; (iv) the Ministry of ICT (now MoDEE), or (v) the Central Bank of Jordan, if the transaction relates to banking or financial operations. See article 34 of the E-transactions law.

The law is also aligned with good practice on ensuring technological neutrality as it does not prescribe a specific form or condition for electronic communications/messages, electronic contracts, or electronic signatures.[54] The definition for the "private key" required to protect qualified e-signatures also appears to be technologically neutral: it is defined in the Law as "a code used to generate electronic signatures for an electronic transaction, information message or electronic document" (Eversheds Sutherland 2020). The law is also technologically neutral in terms of the Certificate Service Provider/Certificate Authority used. This is important to avoid risks of vendor lock-in, bottlenecks to the issuance of trust services, and to ensure the law remains up to date as relevant technologies or new types of providers develop.

In line with the UNCTRAL model laws on e-commerce, certain types of transactions are excluded from the scope of the law. These include transactions to establish and amend a will, establishing "Waqf" and amending its conditions; transactions related to movable or immovable properties requiring registration; powers of attorney and transactions relate to civil status. Additional exceptions in the Jordanian law that are not explicitly provided for in the model laws or other reference documents include notices related to cancelling or revoking contracts for utilities (electricity and water), health insurance and life insurance; court proceedings, judicial notification and court resolutions; and securities.[55]

In 2017, the Jordanian Cabinet approved the e-payment and transfer bylaw to further support the enabling environment for secure e-transactions (Jordan Times 2017). The bylaw sets out requirements and conditions for the licensing of e-payment systems and providers, as well as the types of transactions for which licensed providers can issue certificates and trust services. The regulations also set out the procedures that should be undertaken to settle disputes between parties to an electronic money transfer. (An in-depth assessment of the e-payments bylaw is beyond the scope of this study.)

To support enforcement of the legal framework for e-commerce/e-transactions, the 2015 law specifies the institutional arrangements for undertaking the relevant regulatory and licensing functions. The mandates appear to be divided between MoDEE and the TRC on a sectoral level, with TRC being responsible for the regulation of Cloud infrastructure and services. In terms of e-signature, a key enabler of e-transactions/e-commerce, MoDEE is the root certifier for the public key infrastructure (PKI) and is responsible for issuing e-signatures for G2G services. The TRC is responsible for licensing and regulating certificate providers for G2B/G2C and B2B services. The Central Bank of Jordan (CBJ) appears to be responsible for setting standards and auditing of the Certificate Authorities (CAs). According to Article 34 of the e-transactions law, both public and private entities are authorized to issue digital certificates, which is an important enabler in scaling up and mainstreaming the use of digital signatures in the country. However, no licenses have been issued for Certificate Authorities to date.[56] Similarly, no certificates appear to have been issued for digital signatures (protected or authenticated e-signatures). Despite the relatively robust legal framework, the lack of practical implementation is a bottleneck to e-transactions uptake.

Unlocking the Potential of Data Value

While Jordan seems to succeed in adopting advanced data policies, it is currently lagging in terms of actual implementations to drive value through data. While some data-driven public and private services are emerging, achieving the aspiration of policymakers is not yet fully realized in practice. To date, there is limited clarity on the national guidelines in place or public fora to determine and highlight the different needs and challenges of local data-driven services and products. Some progress has recently been made in this regard. MoDEE has conducted initial public consultations with the private sector and civil society to determine which datasets hold more value and which the government should open first. Citizens can also ask for specific datasets to be opened and published through the e-government portal. These efforts should be systematized to ensure that the GoJ moves from improving access to data to increasing its usage, which is facilitated when data is prioritized and provided with sufficient quality and granularity to meet user needs. Jordan owns a relatively modern infrastructure and has worked intensively to adopt new policies for open data and data classification. Greater value from data is expected to be harnessed once the current obstacles are overcome.

[54] UNICTRAL's Model Law on Electronic Commerce of 1996 also promotes the principle of technological neutrality in the treatment of electronic documentation.

[55] Article 6 of the Law No.15 of 2015. See also Eversheds (2020).

[56] According to an interview with the Telecommunications Regulatory Commission in February 2020. See also research by the World Bank that confirms no certification authorities existed in Jordan as of March 2020 (Molinuevo and Daza Jaller 2020).

By and large, rates of use and sharing of government data by the private sector are low, as companies tend to create and collect their own data to meet their needs. Government-to-business (G2B) data sharing is often limited and no MOUs with government entities have been agreed upon to date. Bottlenecks to the uptake of public sector data by end users is due to the insufficiency or lack of uptake of public sector data by the private sector, the lack of availability of high-value datasets, and companies having difficulties in obtaining data owned by public entities, as many datasets are classified too conservatively as sensitive or secret at the working level. For more data to be re-used, practical advancements in data infrastructure and safeguards need to be adopted. While the GSB, for example, allows for some G2B data transfers, the uneven implementation of the data classification scheme developed by MoDEE, allowing for additional public datasets to be published, currently limits access to government data. The current data infrastructure also poses some challenges: for example, the Open Government Data portal does not provide APIs for mobile apps and web services to interact automatically with the government's data infrastructure and continuously transfer data and updates. This feature is a key enabler in the development of products and services that rely on real-time data, such as meteorological or transport data.

Civil society, universities and research institutions also need more access to data. As the current usage of open datasets available on Jordan's open government data portal is still minimal[57], research institutions, civil society organizations, data journalists and other information intermediaries are facing the substantial challenges of finding and obtaining datasets to analyze. Nevertheless, some coherent and enduring products and services have begun to emerge through the cooperation of a few government entities and the private sector.

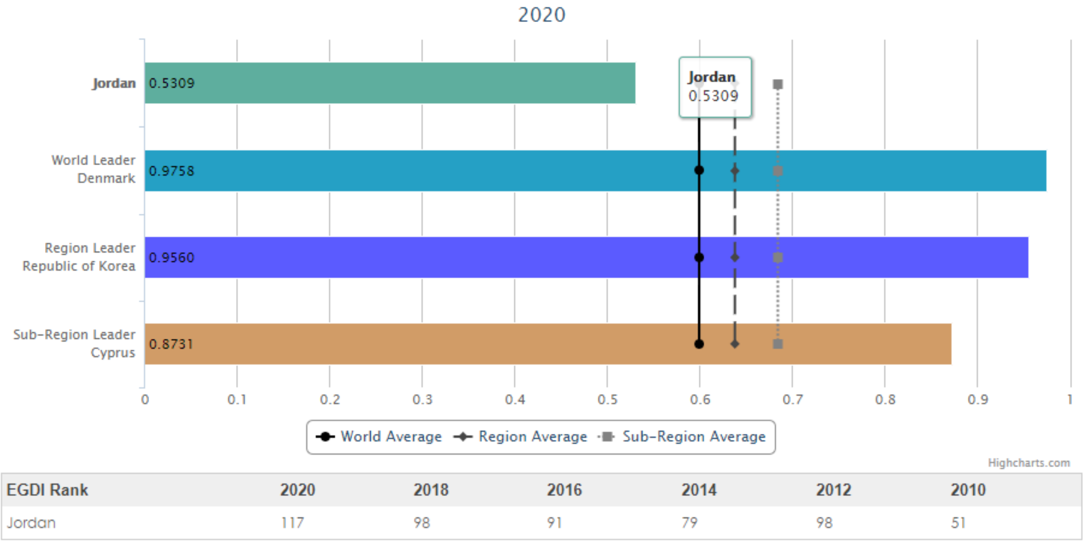
Public Sector-led Data Services

Jordan is a pioneer in initiating e-government in the region. Government e-services offerings have expanded significantly, from just 15 in 2003, to 55 in 2009 and 125 services in 2018. However, Jordan is catching up with other regional peers by expanding its digital government platform and services to support the country's mid-term development strategy. A new digital government plan (2020-2022) is promising to add more than 500 e-services to the government portfolio. This evolving government platform and set of services is reinforced by the adoption of a single sign-on and digital signature as well as a user-centric approach.

As new e-government services are launched, more citizens are benefiting. The catalogue of Jordan's e-government lists 275 different services offered by public entities to citizens and businesses, of which the usage increases constantly. For the first time, the number of monthly transactions for these services exceeded one million in January 2020, almost a threefold increase from 2018. Nevertheless, it is difficult to determine how successful the usage of data has been in these e-services and evaluate whether they are sufficiently user-centered and inclusive. Jordan has fallen back 19 ranks on the United Nations 2020 E-Government Development Index (EGDI), compared to its previous ranking in 2018. The country ranked 117th globally out of 193 countries, while it ranked 10th among the 20 Arab countries covered in the report. Jordan's e-government has regressed on the three main indicators: e-government online services index (OSI), the telecommunications infrastructure index (TII) and the human capital index (HCI). While the country showed some traction on HCI, the country scored one of the lowest progress in Asia about government data use for online services (OSI).

[57] In Jordan, a low impact (that is, a social and economic score of just 6 out of 100) is reported in the latest edition of the Global Open Data Barometer (https://opendatabarometer.org/4thedition/regional-snapshot/middle-east-north-africa/).

Figure 2.5.: UN E-Government Development Index 2020 (EGDI rank)



EGDI Rank	2020	2018	2016	2014	2012	2010
Jordan	117	98	91	79	98	51

Source: UN 2020

The government is promoting the digitalization of cross-government services in which data is transferred in the back office between multiple entities, as they have a more substantial impact on citizens by reducing the administrative burdens a citizen would face if these services were provided separately offline. Interestingly, the first batch of fully digitalized and online-only services provided by the government in 2017-2018 largely consisted of services whose implementation required cross-agency cooperation and data transfers that might have had a positive effect in their adoption. A significant example could be the online service to obtain a non-criminal certificate, provided by the Ministry of Justice, in which the whole process was re-engineered to introduce a smooth and user-friendly experience, while enhancing the behind-the-scenes coordination between the Ministry of Justice, the Public Security Directorate, local carriers and online payment systems. This service was the second-most used within six months of its launch, with more than 200,000 requests in the second half of 2018. As each public entity retains ownership of the data it manages, other successful cross-government examples might arise if whole-of-government resolutions for data re-use and sharing between entities are implemented. According to MoDEE, one of the reasons Jordan has scored low in the United Nations' E-Government Survey is the lack of unified standards for policies and technologies of digital transformation.

Government "big data" has begun to be an important pillar in Jordan's digital government transformation. The latest digital policy considers the use of big data in the public sector to improve analysis, forecasting, and operational performance, and although it states that facilities for sharing data between applications have already been developed, the lack of common standards is an obstacle to the creation and maintenance of big datasets. No prominent examples of big data in the public sector were highlighted, but rather a centralized repository of the National Unified Registry (NUR), a database created to target social assistance and built through the consolidation of datasets previously stored at different entities, including taxation and payroll data and databases of different government agencies, formal private sector workers, pensioners, military, data on beneficiaries of the National Aid Fund (NAF), property and vehicle registration database and the civil registry database.

Going forward, a whole-of-government approach will be critical to facilitate the exchange and transfer of data within the Government and with end users. This approach will also help address any overlap in the roles regarding government open data sharing played by MoDEE and the Department of Statistics (DOS)[58] for example. While the government has already implemented national e-government strategies more cohesion and coordination between government departments remains a work-in-progress in order to maintain smooth data flows and interoperable datasets and deliver on the new plan's aspirations for increasing value of public data.

[58] http://dosweb.dos.gov.jo/

Private Sector-led Data Services

Jordan has the potential to nurture a well-developed digital ecosystem for data-driven innovation within the private sector. Several technology firms, global players, investors, venture capitalists and accelerator incubators operate in the country. The sector's GDP contribution peaked at 12 percent in 2015 (according to Innovative Jordan - https://innovative.jo/ict/). This relatively vibrant ecosystem also benefits from a well-educated digitally trained workforce available within the market as many graduates also have strong industry focused skills required for advancing digital economy (for example, e-commerce, digital financial services, etc.).

Access to government data is crucial to the success of some private sector companies. The ability to obtain and use data owned by public entities is extremely important for the business models of several enterprises in the Jordanian economy. Qistas, for instance, has digitized most of Jordan's case law after an agreement with the Ministry of Justice, and provides access to a collection of past legal decisions written by courts under a subscription model. Additionally, government data could require additional extensive processing to acquire more economic value, as in the case of KINZ, the first company in Jordan to specialize in corporate data mining with a database consisting of more than 120 thousand companies. In addition to data cleansing, KINZ was one of the companies that leveraged different data sources to introduce new services, like sales lead management and reporting. These examples show that new businesses can arise and thrive if public data is accessible. Additional opportunities can be unlocked by making more data available.

Jordan's different economic sectors can benefit from more access to public data. Although the usability, relevance and quality of publicly available datasets provided by the Government has led to little value creation in the private sector so far, partnerships and synergies between public institutions and the private sector provide examples of services and enterprises built on data. An example that is frequently highlighted is the private, non-profit company, Electronic Health Solutions (EHS) that, since 2009, is responsible for digitizing the public healthcare sector in Jordan. It operates the Hakeem program which resulted in the automation of more than 195 health entities nationwide with more than 7 million electronic medical files. In 2019, EHS launched a health data analytics program, HDA, to support researchers and decision-makers in the health sector with reliable information using data mining tools.

Jordan's private sector and technology startups are moving at a faster pace than the public administration in embracing the data economy. Public-Private Partnerships (PPPs) could be significant enablers to create additional value from data. In this regard, the Central Bank of Jordan (CBJ) emerges as a front-runner in terms of data quality and the initiation of regulatory sandbox. JOPACC, owned by the CBJ along with the 24 banks operating in Jordan, is an illustrative example that appears to be the main functional digital financial payment system in the country.

Digital financial services and emerging fintech companies heavily depend on data. Alongside CBJ, traditional banking institutions have initiated promising fintech initiatives. For instance, Arab Bank launched a US$30 million venture fund targeting fintech with special focus on technologies like artificial intelligence and machine learning, in addition to a 950 square meter 'innovation hub' and an accelerator program. Ahli Bank, through its subsidiary Ahli Fintech, has also launched an accelerator and provides a sandbox environment. In addition to payment service MadfooatCom, other fintech startups are emerging, like lending platform Liwwa that utilizes machine learning for credit assessment, credit scoring and benchmarking.

Additional examples of data innovation are emerging from Jordan's ICT and technology startup ecosystem. Comprising more than 600 technology companies, of which at least 300 are startups, many enterprises provide innovative services or products based on the data value chain. The following are some examples:

- **MeteoWeather,** a Jordanian startup that invested heavily in the collection and analysis of meteorological data. Using artificial intelligence (AI) models, they were able to introduce numerical predictions, decision support systems and APIs to provide access to their datasets;

- **IrisGuard** developed innovative technologies that allowed 1.5 million refugees to use digital money using a scan of their irises instead of cash;

- **OpenSooq** also leverages AI and machine learning (ML) intensively for different aspects of their e-commerce platform and its supporting services and moderation tools;

- **Nestrom** provides a platform for data collection through various means, including IoT sensors from field operations, delivering business and performance insights through data analysis;

- **Whyise** is an impact analytics startup that allows organizations to aggregate data in real-time and analyze them based on different standards to take evidence-based decisions. Both Whyise and Nestrom companies received investments from the Jordanian venture capital firm Propeller.

Jordan is becoming distinguished in the field of Arabic natural language processing (NLP) and activities related to the processing of Arabic textual data. The country has always been one of the major contributors of Arabic online content. Mawdoo3 is a content publisher that developed unique NLP tools for its AI-powered Arabic speaking digital assistant, and it has recently secured a total of $23.5 million in funding to develop its AI-supported digital platform Ujeeb. Jordanian companies Arabot and Labiba have developed sophisticated NLP technologies to provide innovative Arabic 'chatbot' solutions in the region. Other data-driven companies are operating in Jordan. Logistics provider Aramex, for example, has turned to AI, automation and innovative technologies to become a fully data-driven organization. Other international companies, like the e-commerce Souq.com which was acquired by Amazon in 2017, have a significant data science team in its office in Amman.

The need for data is also pushing significant changes in the academia and skilled workforce. As different companies operating in Jordan are demanding skilled personnel to be recruited into the different data-driven job opportunities in the private sector, local universities have initiated new STEM programs to maximize the local pool of talents. Both Princess Sumaya University for Technology (PSUT) and Jordan University of Science and Technology (JUST) offer a postgraduate degree in Data Science, and other institutions are offering bootcamps and training courses in Data Science and AI.

3. Recommendations for More Effective Data Governance in Jordan

Data governance and data-centric policymaking are becoming a strategic imperative. With a modern digital infrastructure and a growing technological capacity to process large and complex datasets, the potential and opportunities surrounding data abound in Jordan. Policymakers can have better insight and foresight, government entities can deliver more efficient and inclusive e-services, and the private sector can create innovative products and services.

Jordan has made a strong policy commitment to digital transformation. There are several regulations in place to provide guidance and assign roles and responsibilities, mainly for digital government development and transformation. MoDEE is designated as the lead agency in facilitating the implementation across government ministries, departments, and agencies. Although there is an institutional framework and setting to advance such implementation, limited clarity on a national overarching implementation strategy, matched by adequate resources, hinders the Government from advancing at an appropriate pace with digital government and transformation.

Specifically, the Government could further enhance current progress and strengthen its commitment towards developing a robust data governance framework through the following initiatives:

Enabling data infrastructure

A continued investment in modern data infrastructure remains a key enabling foundation for advancing the implementation of a robust data governance ecosystem in Jordan. The COVID-19 crisis has propelled the need for digital transformation in the country, and the Government is dealing with a large increase in the volume, variety and velocity of data transactions and a growing need for data-driven products and services.

The simple upgrade of current infrastructure and systems will be insufficient to ensure that this ever-increasing quantity of data remains accessible. It also crucial to ensure that such large volumes can be shared, used and analyzed efficiently. The recent adoption of a national cloud computing policy is a step forward; accelerating the transition to cloud infrastructures is becoming a necessity with the fast increase in government data. An expansion of the Jordanian national cloud initiative is expected to unlock the value of big data and foster scientific and technological innovation while helping achieve the objectives of the country's digital transformation. The Government and the regulator (TRC) can consider public-private cloud infrastructure partnerships (CORDIS 2020) to enhance the availability and capacity of appropriate data infrastructure.

The expansion of 5G deployment in the next few years will open new opportunities for data flows. This will require careful considerations of managing the personal data involved. The development and adoption of a smart data protection law that encourages Privacy-by-Design and is technology neutral will be critical to effectively mitigate new data protection risks. In this regard, Jordan can provide a leading example in the region for an open, inclusive discussion regarding 5G and data protection that can benefit citizens and businesses, most of all the individuals whose data may be collected and processed.

Beyond hard infrastructure, it will be essential for the GoJ to continue supporting the development and standardizing the implementation of a robust set of unified standards for data interoperability. In this vein, the effective implementation of harmonized standards for data classification remains limited despite the existence of a data classification policy. Despite MoDEE's efforts in pilot training at the working level, there is still restricted application of the government data classification framework. As data needs continue to increase, processing and storing vast - and theoretically unlimited - amounts of data without a purpose and user needs-driven practice of data management and classification across the public service will be unsustainable and not lead to increased uptake by end users.

Finally, authentication is an essential step in the provision of services and access to data. Jordan's Ministry of Interior and MoDEE have rolled out an ambitious citizen ID program (Thales 2018). Digital identity plays a central role in data applicability as it provides the foundation on which data can be safely and securely shared within and between agencies. The system proved its value during the COVID-19 crisis as it offered a range of innovative services transforming the way the public interacts with the state. An expansion of digital identity authentication will enable more users to safely access services and data (Pangestu 2020).

Supporting institutional leadership, coordination and capacity building

The Government has a leading role in formulating and activating comprehensive policies and legislation to support data governance. The challenge remains in enforcement and implementation. As illustrated in the analysis findings, there are several appropriate laws governing access to information, personal data protection, open government data, e-commerce/e-transactions, as well as data interoperability, emerging technologies and related applications.

A holistic and Whole-of-Government approach to data governance is required in pursuit of accelerating data-enabled digital transformation and advancing a digital economy in Jordan. The central feature of such an approach is the alignment of institutions, organizations, technology and resources to support the desired changes within and outside the public sector for the generation of value through data. Several governments have adopted such a horizontal and integrated approach by promoting both organizational and technological interoperability, for example to improve the efficiency of public services delivery. Singapore has adopted a holistic approach for its Smart Nation program (Government of Singapore 2021). It has moved from a silo-based approach to an ecosystem approach in which data flows and is exchanged effectively within a robust legislative and regulatory environment. Other examples come from the United Arab Emirates (UAE) and Estonia (World Government Summit 2019) where Governments are using different technologies and data on their platforms to anticipate the needs of citizens through predicted and personalized services in simplified life events and citizen journeys. For example, once a birth is recorded in the civil registry, parents get automatic notifications and updates on vaccinations and childcare information.

In the era of data revolution, a shift in the evolving role of the Telecommunications Regulatory Commission (TRC) is a necessity in Jordan. From a gatekeeper and arbiter in the telecommunications sector, TRC role is to help enable data sharing and facilitate regulatory sandboxes for maximizing value from data use. An emphasis on "collaborative regulation" will be critical for the regulator to work with other stakeholders in the digital and data ecosystems (ITU 2020). This approach can be applied when putting in place measures such as sandboxes and 5G pilot projects to promote data-driven innovation.

While the fundamental policy, legal and regulatory build up for data governance have been put in place under the leadership of MoDEE, implementation of these frameworks has been uneven. The legal framework for e-commerce/e-transactions for example has been in place since 2015, but no licenses for certificate agencies have been issued. Similarly, while the framework for cybersecurity includes a strategy, policy, and both a cybersecurity and cybercrime law, its effective implementation remains limited by a lack of institutional anchoring and capacity at the strategic and operational layers. In other instances, overlaps in institutional mandates on certain portfolios, such as between MoDEE and the Department of Statistics (DOS) in the area of Open Data, have implications for the success of reform implementation.

Through collaboration, national stakeholders can develop standards to enable the access, use and reuse of government data in Jordan. MoDEE can coordinate with the Department of Statistics (DOS) and other public sector entities that play a significant role in collecting and using administrative and statistical data (for example, the Ministry of Economy). The focus is to be on ensuring that these standards are developed in a consultative manner to be informed by the needs of end users. Therefore, the design process led by the Government should also be undertaken in collaboration with civil society and the private sector following a multi-stakeholder approach to data governance. Through public engagement, public openness can be promoted not only in the use and sharing of government data, but also in the development and regulation of services that are dependent on data (Rempel et al. 2018).

An essential component of the Government's collaborative role is the provision of opportunities for public and private stakeholders to drive data innovation and create value. By empowering specialists to leverage available datasets (big data, open data, geospatial data, real-time data, etc.), the Government can enable opportunities for leapfrogging in areas such as provision of new public services and the development of smart cities (Petra 2020). Regular events for crowdsourced data processing and Open Government Data hackathons can be beneficial for driving further data innovation. MoDEE, in cooperation with TRC, can also adopt an experimental approach to policy design (that is, regulatory sandboxes) to validate the impact of variations in more enabling policies and regulations. This can support easing the feasibility and scalability of deploying new emerging technologies for generating data-centric value (for example, use of artificial intelligence and/or blockchain) while remaining committed to safeguarding privacy.

The Way Forward

Data governance is rapidly moving towards becoming a strategic imperative in Jordan. Enhancing the use of government data can increase the productivity and accountability of public institutions while providing the private sector with more opportunities for creating data innovation. Jordanian policymakers and regulators can leverage data to inspire public trust. The COVID-19 crisis has created an opportunity to accelerate the country's digital transformation. However, the full potential of this transformation will only be realized when the Government can bridge data gaps, integrate data related policies and systems, and implement them with the appropriate safeguards for security and privacy.

This country case study has its limitations. The analysis has mainly focused on data which the government controls and barely delves into personal data within the private sector (enterprises and operators). Additionally, the governance of cross-border data transactions, an increasingly critical areas for developing Jordan as a digital hub, would benefit from further exploration and in-depth analysis. Additional research on supply and demand for cloud services could be useful in identifying the capacity and investment needs for new cloud infrastructure and services.

To enable a more effective data governance in Jordan, three proposed areas of focus are highlighted. The three areas are based on the recognition that there is a reasonably robust foundational policy and regulatory framework in place, but standards have not been consistently harmonized and adopted across the whole government, creating challenges for the uptake of data by end users. The first area focuses on the current limitations of the government data infrastructure (MoDEE) but links these to the broader value chain. The second relates to enhancing the enforcement of data-related policies, laws and regulations that enable trusted use and data sharing and protect personal data and the rights of data subjects. Thirdly, the emphasis is on institutional leadership, coordination and capabilities to strengthen executive abilities, resource availability and the whole-of-government approach to implementation. A few critical actions are suggested to act on within a three-year implementation time span: short term (1-12 months); medium-term (12-24 months), and long-term (24-36 months).

Adoption of a national government interoperability plan

Table 3.1. Challenges to address within 3 years

Data-related challenges to be addressed	Short-term (1-12 months)	Medium-term (12-24 months)	Long-term (24-36 months)
1. Government data infrastructure limitations (*e.g.,* architecture; G-Cloud; API standards; network security; etc.)	Finalize adoption of a national cloud policy with clear security standards and certification	Adopt a national government interoperability plan. Address infrastructure investment required to achieve 2030 target.	Develop a new "smart government" strategy that is user-centric and data-driven. Expand Implementation of data infrastructure required.
2. Limited adoption and/ or enforcement of key legislative and regulatory frameworks enabling trusted data use and sharing	Adopt a revised Data Protection and Privacy Law to regulate the collection and processing of personal data (including by Government) in line with international good practice	Adoption of implementing regulations for the data protection law	Enhance the independence and capability of a data protection agency to support enforcement of the data protection law (guide and clarify standards, enforce, monitor, and provide redress)

Data-related challenges to be addressed	Short-term (1-12 months)	Medium-term (12-24 months)	Long-term (24-36 months)
3. Weak organizational and institutional **leadership, coordination, and capabilities**	Adoption and implementation of unified standards for classification, sharing and usage of datasets. Enhance the human capital and skills needed in the public sector to implement data-related policies.	Binding policy or regulation defining standards and governing usage of metadata, anonymized data and tagged data (e.g., geo-locations) across the whole-of-government.	Policies and Regulations that enable government entities to securely transfer data across borders and use of processing in secured Data warehouses.

Source: World Bank

An effective data ecosystem is driven by a dynamic relationship between policies, institutions, people, regulations and enabling data infrastructure. Jordan presents an illustrative case on how these elements intersect to create opportunities and challenges for harvesting public value from data. An effective data governance regime requires a long-term ecosystem approach that takes into consideration an evolving data security and privacy landscape.

References

Access Now. 2019. “Cybercrime law in Jordan: pushing back on new amendments that could harm free expression and violate privacy.” February 19. https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/

Article 19. 2005. “Memorandum on Jordan’s Protection of State Secrets & Documents Provisional Law No. (50).” London, England. https://www.refworld.org/pdfid/475e4e400.pdf

Barton, James. 2020. “Jordan’s regulator takes credit for ‘improvement’ during pandemic.” Developing Telecoms. June 16. https://www.developingtelecoms.com/telecom-business/telecom-regulation/9654-jordan-s-regulator-takes-credit-for-improvement-during-pandemic.html

CORDIS. 2020. “Infrastructures PPP for a Smart Connected Future (2020): A European ICT Industry Initiative for Horizon 2020.” https://cordis.europa.eu/docs/projects/cnect/5/317105/080/deliverables/001-InfrastructuresPPP.pdf

CJEU (Court of Justice of the European Union). 2020. “Judgment in Case C-311/18: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield.” Press release No. 91/20, July 16. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

Eversheds Sutherland. 2020. “Electronic signatures in Jordan.” April 26. https://www.eversheds-sutherland.com/global/en/what/publications/shownews.page?News=en/middle-east/jordan/Electronic_signatures_in_Jordan.

Government of Singapore. 2021. “Transforming Singapore Through Technology.” Smart Nation and Digital Government Office. https://www.smartnation.gov.sg/

GSMA. 2020. “5G and data privacy: an overview for policy makers.” https://www.gsma.com/publicpolicy/wp-content/uploads/2020/07/GSMA_5G_and_Data_Privacy_July_20.pdf

ITU (International Telecommunication Union). 2020. Global ICT Regulatory Outlook 2020. Geneva, Switzerland: ITU Publications. https://www.itu.int/pub/D-PREF-BB.REG_OUT01.

Jordan Investment Commission (JIC). 2020. “Jordan and ICT Environment.” https://www.jic.gov.jo/en/ict/#:~:text=-Jordan%20and%20ICT%20Environment

Jordan Times. 2017. “Cabinet approves e-payment by-law.” October 23. https://www.jordantimes.com/news/local/cabinet-approves-e-payment-law

Jordan Times. 2019. “TRC invites telecom companies for 5G trial.” September 16. https://www.jordantimes.com/news/local/trc-invites-telecom-companies-5g-trial

Lomas, Natasha. 2020. “Facebook told it may have to suspend EU data transfers after Schrems II ruling.” TechCrunch. September 9. https://techcrunch.com/2020/09/09/facebook-told-it-may-have-to-suspend-eu-data-transfers-after-schrems-ii-ruling/

MEI (Middle East Institute). 2020. “Jordan adopts sweeping cybersecurity legislation.” January 30. https://www.mei.edu/publications/jordan-adopts-sweeping-cybersecurity-legislation

MoDEE (Ministry of Digital Economy and Entrepreneurship). 2019. Data Classification & Management Policy (2019). https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/EB_List_Page/Data_management_and_classification_policy.pdf

MoDEE (Ministry of Digital Economy and Entrepreneurship). 2020. Jordan Digital Transformation Strategy 2020a. https://www.modee.gov.jo/EBV4.0/Root_Storage/EN/1/Jordan_Digital_Transformation_Strategy_2020_English_Unofficial_Translation.pdf

MoDEE (Ministry of Digital Economy and Entrepreneurship). 2020b. Cloud (Platforms & Services) Policy 2020. https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/cloudpolicy-2020-english.pdf

MoDEE (Ministry of Digital Economy and Entrepreneurship. 2020c. "National Broadband Network Program." https://www.modee.gov.jo/EN/Pages/National_Broadband_Network_Program

MoICT (Ministry of Information and Communications Technology) and INT@J (Information and Communications Technology Association - Jordan). 2016. REACH2025: Jordan's Digital Economy Action Plan. http://www.reach2025.net/

MoICT (Ministry of Information and Communications Technology). 2018. General Policy For The Ict And Postal Sectors 2025. http:// وزارة-الاتصالات-وتكنولوجيا-المعلومات.الاردن/uploads/Public-Consultations/ICTP%20Policy%202025.pdf

MoPIC (Ministry of Planning and International Cooperation). 2018. The Fourth National Action Plan 2018 – 2020 Under the Open Government Partnership Initiative (OGP). https://www.opengovpartnership.org/wp-content/uploads/2019/01/Jordan_Action-Plan_2018-2020.pdf

Molinuevo, Martin, and Lillyana Daza Jaller. 2020. "Digital Trade in MENA: Regulatory Readiness Assessment." Policy Research Working Paper 9199, Office of the Chief Economist, Middle East and North Africa Region, World Bank Group. http://documents1.worldbank.org/curated/en/786271585574266618/pdf/Digital-Trade-in-MENA-Regulatory-Readiness-Assessment.pdf

OECD (Organization for Economic Co-operation and Development). 2013. The OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD (Organization for Economic Co-operation and Development). 2019a. "Using digital technologies to improve the design and enforcement of public policies." OECD Digital Economy Papers, No. 274. Paris, France: OECD Publishing. https://doi.org/10.1787/99b9ba70-en .

OECD (Organization for Economic Co-operation and Development). 2019b. "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies." https://www.oecd-ilibrary.org/sites/276aaca8-en/index.html?itemId=/content/publication/276aaca8-en

Pangestu, M. 2020. "Harnessing the power of digital ID." Jordan Times, August. http://www.jordantimes.com/opinion/mari-pangestu/harnessing-power-digital-id

Petra (Jordan News Agency). 2020. "USTDA and Greater Amman Municipality Partner to Advance 'Smart Cities' in Jordan." Press release, September 30. https://petra.gov.jo/Include/InnerPage.jsp?ID=10592&lang=ar&name=en_news

Rempel, E., J. Barnett and H. Durrant. 2018. "Public engagement with UK government data science: propositions from a literature review of public engagement on new technologies." Government Information Quarterly, Vol. 35, No. 4, 569-578. http://orca.cf.ac.uk/117261/

Sunlight Foundation. 2017. "Ten Principles for Opening Up Government Information." https://sunlightfoundation.com/policy/documents/ten-open-data-principles/

Thales. 2018. "Jordan launches its new national ID card program." https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/national-id-card-jordan.

UN (United Nations System). 2018. Personal Data and Privacy Principles. Chief Executives Board for Coordination. https://www.unsystem.org/personal-data-protection-and-privacy-principles

UNCITRAL (United Nations Commission on International Trade Law). 1998. "Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998." https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

UNCITRAL (United Nations Commission on International Trade Law). 2001. "Model Law on Electronic Signatures." https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

UNCTAD (United Nations Conference on Trade and Development). 2016. United Nations Guidelines for Consumer Protection. https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf

UNCTAD (United Nations Conference on Trade and Development). 2017. Guidelines on Consumer Protection: Agency Structure and Effectiveness. MENA Programme.

UN DESA (United Nations Department of Economic and Social Affairs). 2020a. E-Government Development Index (EGDI). https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index.

UN DESA (United Nations Department of Economic and Social Affairs). 2020b. 2020 United Nations E-Government Survey. https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey

UN ESCWA (United Nations Economic and Social Commission for West Asia). 2019. "Jordan: Open Government and Open Data." Workshop agenda, March 24-25. https://www.unescwa.org/events/workshop-national-open-government-data-jordan

World Bank. 2018. Mashreq 2.0: Digital Transformation for Inclusive Growth and Jobs. Washington, DC. https://www.worldbank.org/en/country/jordan/publication/mashreq-20-digital-transformation-for-inclusive-growth-and-jobs.

World Bank. 2019. "Amman Communique: The First Digital Mashreq Forum." Press release, June 29. https://www.worldbank.org/en/news/press-release/2019/06/30/amman-communique-the-first-high-level-mashreq-conference-on-digital-transformation-commitments

WEF (World Economic Forum) and Bain & Company Inc. 2011. Personal Data: The Emergence of a New Asset Class. Geneva, Switzerland: WEF. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_ 2011.pdf

WEF (World Economic Forum). 2015. Data-Driven Development: Pathways for Progress. Advisory Group on a Data Revolution for Sustainable Development. http://www3.weforum.org/docs/WEFUSA_DataDrivenDevelopment_Report2015.pdf

World Government Summit. 2019. "Shaping the data economies of the future". Dubai, UAE. Available at: https://www.worldgovernmentsummit.org/observer/reports/2019/building-the-data-economies-of-the-future

MENA
TECH
Unlocking Digital Transformation

AN INITIATIVE OF
WORLD BANK GROUP