WEST BANK & GAZA
DATA GOVERNANCE
FRAMEWORK ASSESSMENT

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

KoDi
Accelerating Digital Transformation
Disclaimer

© 2023 International Bank for Reconstruction and Development / The World Bank

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.

The West Bank & Gaza Data Governance assessment is designed to support a qualitative landscape or modular analysis of the country's existing data policy, legal and regulatory framework, and practices that enable the effective and trustworthy usage of data for economic development purposes. While the assessment covers key areas of the enabling policy legal and regulatory environment, in-depth diagnostics of each dimension covered in the assessment are beyond the scope of this report. The assessment (and its underlying diagnostic framework, the Toolkit) is based on evolving international good practice, including in emerging areas where regulatory regimes are either nascent or unsettled. As an assessment framework, it is intended as a basis for broad, multistakeholder consultation on what the Palestinian Authority may consider including in its infrastructure, policy, legal and regulatory and institutional framework.

This report is based on version 3.0 of the Toolkit, which is a living document, and is intended to be updated from time to time. The information in this report is current as of February 2023. All references to treaties, policies, laws, regulations, and standards recognize that these may be reversed, repealed, amended, etc. over time.

There is no guarantee that addressing all the issues raised in the assessment framework (Toolkit) and Report will result in a perfect or even workable enabling environment for data regulation in a country, which can be affected by exogenous factors that differ depending on political economy, economic and other constraints.

Images: Shutterstock.

Rights and Permissions

The material in this work is subject to copyright. Because the World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for non-commercial purposes as long as full attribution to this work is given. Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, the World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>10</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>17</td>
</tr>
<tr>
<td>SCOPE OF THE ASSESSMENT</td>
<td>20</td>
</tr>
<tr>
<td>LEADERSHIP</td>
<td>20</td>
</tr>
<tr>
<td>Digital transformation, Digital economy, Digital government</td>
<td>20</td>
</tr>
<tr>
<td>Data for decision-making, Open data</td>
<td>21</td>
</tr>
<tr>
<td>Open government, Transparency, Accountability</td>
<td>22</td>
</tr>
<tr>
<td>Data security</td>
<td>22</td>
</tr>
<tr>
<td>Personal data protection</td>
<td>23</td>
</tr>
<tr>
<td>Coordination mechanisms</td>
<td>23</td>
</tr>
<tr>
<td>Conclusion</td>
<td>24</td>
</tr>
<tr>
<td>ENABLERS: ENABLING DATA TRANSACTIONS/FLOWS AND (RE)USE OF DATA</td>
<td>25</td>
</tr>
<tr>
<td>Access to information</td>
<td>25</td>
</tr>
<tr>
<td>Data classification</td>
<td>29</td>
</tr>
<tr>
<td>Open data</td>
<td>31</td>
</tr>
<tr>
<td>National statistical system</td>
<td>36</td>
</tr>
<tr>
<td>E-Government framework</td>
<td>39</td>
</tr>
<tr>
<td>E-Transactions</td>
<td>44</td>
</tr>
<tr>
<td>SAFEGUARDS: TRUST IN DATA FLOWS AND THE (RE)USE OF DATA</td>
<td>47</td>
</tr>
<tr>
<td>Personal data protection</td>
<td>47</td>
</tr>
<tr>
<td>Data security</td>
<td>49</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>52</td>
</tr>
<tr>
<td>STAKEHOLDER MAPPING</td>
<td>54</td>
</tr>
<tr>
<td>PROPOSED ACTION PLAN</td>
<td>57</td>
</tr>
<tr>
<td>ANNEX I: SUMMARY OF PROPOSED ACTION PLAN</td>
<td>71</td>
</tr>
<tr>
<td>ANNEX II: METHODOLOGY</td>
<td>72</td>
</tr>
<tr>
<td>ANNEX III: GLOBAL REGULATION TOOLKIT QUESTIONNAIRE USED IN THIS ASSESSMENT</td>
<td>74</td>
</tr>
</tbody>
</table>
### LIST OF ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>ATI</td>
<td>Access To Information</td>
</tr>
<tr>
<td>CoM</td>
<td>Council of Ministers</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CDO</td>
<td>Chief Data Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CSO</td>
<td>Civil Society Organization</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>FCV</td>
<td>Fragility, Conflict, and Violence</td>
</tr>
<tr>
<td>ECG</td>
<td>E-government Core Group</td>
</tr>
<tr>
<td>ESCWA</td>
<td>United Nations Economic and Social Commission for West Asia</td>
</tr>
<tr>
<td>G2B</td>
<td>Government to Businesses</td>
</tr>
<tr>
<td>G2C</td>
<td>Government to Citizens</td>
</tr>
<tr>
<td>G2G</td>
<td>Government to Government</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>M&amp;E</td>
<td>Monitoring and Evaluation</td>
</tr>
<tr>
<td>MDA</td>
<td>Ministries, Departments, and Agencies</td>
</tr>
<tr>
<td>MoE</td>
<td>Ministry of Education</td>
</tr>
<tr>
<td>MoHE</td>
<td>Ministry of Higher Education</td>
</tr>
<tr>
<td>MoF</td>
<td>Ministry of Finance</td>
</tr>
<tr>
<td>MoH</td>
<td>Ministry of Health</td>
</tr>
<tr>
<td>MoI</td>
<td>Ministry of Interior</td>
</tr>
<tr>
<td>MoLG</td>
<td>Ministry of Local Governorate</td>
</tr>
<tr>
<td>MoM</td>
<td>Ministry of Media/Ministry of Information</td>
</tr>
<tr>
<td>MoTA</td>
<td>Ministry of Tourism and Antiquities</td>
</tr>
<tr>
<td>MTIT</td>
<td>Ministry of Telecommunication and Information Technology</td>
</tr>
<tr>
<td>NADA</td>
<td>National Data Archives</td>
</tr>
<tr>
<td>NDP</td>
<td>National Development Plan</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>NPA</td>
<td>National Policy Agenda</td>
</tr>
<tr>
<td>NSO</td>
<td>National Statistics Office</td>
</tr>
<tr>
<td>NSS</td>
<td>National Statistical System</td>
</tr>
<tr>
<td>ODIN</td>
<td>Open Data Inventory Index</td>
</tr>
<tr>
<td>ODSC</td>
<td>Open Data Steering Committee</td>
</tr>
<tr>
<td>OGP</td>
<td>Open Government Partnership</td>
</tr>
<tr>
<td>PA</td>
<td>Palestinian Authority</td>
</tr>
<tr>
<td>PCBS</td>
<td>Palestinian Central Bureau of Statistics</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PMA</td>
<td>Palestinian Monetary Authority</td>
</tr>
<tr>
<td>PMO</td>
<td>Prime Minister's Office</td>
</tr>
<tr>
<td>RM</td>
<td>Ramallah Municipality</td>
</tr>
<tr>
<td>SDG</td>
<td>Sustainable Development Goals</td>
</tr>
<tr>
<td>SPI</td>
<td>World Bank Statistical Performance Indicators</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>WB&amp;G</td>
<td>West Bank and Gaza</td>
</tr>
</tbody>
</table>
# TERMS AND DEFINITIONS

The table below introduces the key terms used in the document and their definition.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data inventory</td>
<td>A data inventory is a list of data assets collected or produced by an organization.</td>
</tr>
<tr>
<td>Data register</td>
<td>A data register, also known as master data or reference data, is a data resource that contains unique identifiers shared across the government. For example, the population register is a data register that contains the list of unique personal identifiers for all citizens of a country. Common data registers include population registers, businesses registers, and address registers.</td>
</tr>
<tr>
<td>Data sharing at transactional level</td>
<td>This is the type of data sharing that is implemented in e-government infrastructure where an e-service developed by one ministry is able to query in real time an information system hosted at another ministry via a standardized interface.</td>
</tr>
<tr>
<td>Raw data sharing</td>
<td>In contrast with data sharing at transactional level, raw data sharing is the sharing of a bulk of information (a dataset). This data sharing takes place at the initiative of the entity owning the data and consists of publishing the datasets on a (open) data portal to support data analysis and mashups.</td>
</tr>
<tr>
<td>Hukumati</td>
<td>Hukumati—“my government” in Arabic—is the name of the central one-stop-shop portal for all Palestinian Authority (PA) e-government services.</td>
</tr>
<tr>
<td>X-Road/UXP</td>
<td>X-Road (recently renamed UXP) is the name of a platform originally developed by the Estonian government to support data sharing at transactional level. The platform was then released publicly and has been deployed in a number of countries. It is the platform selected by the PA and deployed in Palestine.</td>
</tr>
<tr>
<td>Zinnar</td>
<td>Zinnar is the name of the interoperability framework designed and adopted by the PA. The role of the interoperability framework is to ensure that government agencies agree on vocabulary, meaning, structure, codes, and business rules involved in the sharing of data.</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

The principal authors of this report are Stephane Boyera, Gavin Chait, and Aman Grewal from SBC4D.1 The overall assessment work was performed jointly with the World Bank team, led by Hyea Won Lee (Digital Development Specialist) and comprising Eric Dunand (Senior Digital Development Specialist), Zaki B. Khoury (Senior Digital Development Specialist), Kimberly Johns (Senior Public Sector Specialist), Adèle Barzelay (Counsel, Data, and Digital Development), Issam Khayat (Digital Development Specialist), and Sameeksha Khare (Digital Development Consultant). The team acknowledges the strategic guidance provided by Nicole Klingen (Practice Manager, Digital Development). This work also received contributions from David Satola (Lead Counsel), Malarvizhi Veerappan (Program Manager), and Rong Chen (Economist).

Finally, this diagnostic was conducted with support from and in close coordination with the Ministry of Telecommunication and Information Technology and in particular Eng. Samer Ali, former Project Management Unit Director; Mr. Zuhdi Jarrar; Ms. Rania Jaber; Mr. Ashraf Abdel Hadi; Mr. Youssef Ertahi; and Mr. Abed Khooli, consultant. We would also like to thank the Palestinian Central Bureau of Statistics and in particular Mr. Haitham Zeidan, Mr. Husam Khaleifeh, Ms. Rania Abu Ghaboush, Ms. Rana Al-Kholi and Ms. Haleema Saeed.

The World Bank team further wishes to extend its gratitude and appreciation to all the stakeholders (listed in the Stakeholder Mapping section) for their collaboration in the study. Their input and feedback contributed significantly to this report.

This report was made possible by the Korea Digital Development Program (KoDi).

EXECUTIVE SUMMARY

Public sector data can lead to better development outcomes by improving governance and creating economic activity through supporting business optimization in the private sector and meaningful job creation and also enabling innovation and entrepreneurship. Enhanced data use and sharing can also enhance the efficiency and quality of public services delivery and contribute to informed decision-making in areas such as monitoring public health and resource management for schools. Robust data governance frameworks and a greater use of public sector data are a key element to support the digital transformation of the Palestinian Authority (PA) and the development of the digital economy in the West Bank and Gaza (WB&G).

Data governance and use in settings affected by fragility, conflict, and violence (FCV)—such as the WB&G—have the potential to address development challenges, but the FCV context also places constraints on setting laws, policies, and regulations as well as their effective implementation. While cognizant of the challenges, it is imperative to strive for the development of a data-driven economy, where the increased availability of data-driven public and private sector services is a key opportunity to lower the FCV-related impact of the communication, movement, infrastructure, and physical access challenges that Palestinians experience.

The PA recognizes the benefits of digital transformation and has mobilized resources to develop the digital economy, setting a high-level vision for leveraging data to achieve its development priorities. It has invested in significant facets, such as laying core frameworks for e-government and initiating an open data initiative, which can realize the value of data at scale with the Ministry of Telecommunication and Information Technology (MTIT) at the center. The presence of a solid technical stack with Zinnar and UXP/X-Road interoperability frameworks and the launch of a one-stop-shop portal for e-services (“Hukumati”) serve as key foundations for all ministries, departments, and agencies (MDAs) to access and share data for transactional operations. In particular, Hukumati has ramped up momentum within the MDAs to invest in development and enable e-services to citizens. As the national statistics office, the Palestinian Central Bureau of Statistics (PCBS) invests in the production of national statistics and Sustainable Development Goals (SDG) data. The MTIT and PCBS consider and adopt international best practices and globally recommended tools and approaches in the above-mentioned areas. They perform particularly well on some international indexes, such as Open Data Inventory index (ODIN) and World Bank’s Statistical Performance Indicators (SPI).

However, the potential of data remains largely untapped in the WB&G. While the PCBS is a robust national statistics office producing timely, quality national statistics that have significantly progressed in the last few years, the government’s use of these statistics in decision-making, policymaking, or evaluation is limited. Furthermore, the assessment finds that e-services initiatives are not based on robust data management processes and have not led to developing key data governance frameworks within MDAs. Except for transactional data shared via X-Road/UXP, there is limited data sharing between MDAs. With the exception of specialized MDAs such as the MTIT and PCBS, data are not widely viewed as critical assets, but considered as a technical matter for IT departments with limited capacity in most MDAs. This results in MDAs implementing limited data management practices. For example, no MDA keeps a data inventory, and most do not conduct routine data analysis. The limited capacity further risks the operational continuity of several data systems, which are often maintained by specific individuals who are the only ones with the knowledge to operate and maintain them in the absence of systemic processes for sustaining technical skills and knowledge. The challenge of capacity constraints is further exacerbated by the weak institutional capacity persistent in the WB&G.
Limited data use in the public sector is driven by the following two underlying factors. First, key enabling policy and legal frameworks are absent. Sharing data requires a dedicated legal framework that supports classification of data assets and determines who has access and the method of processing before sharing. The lack of legislation for data classification, personal data protection, and access to information (ATI) inhibits this classification process. In the absence of these components, each MDA defines its own internal procedures, which are not necessarily consistent with others. Second, ad hoc data request procedures hinder data access and use. Owing to the lack of an enabling legal framework for data classification and of a data inventory that would identify available data and state classification categories of data assets, each data request procedure—whether from another MDA or from a non-governmental entity—is long and unpredictable. Each request usually requires ministerial approval, which then is translated into an memorandum of understanding (MoU) and transmitted to the IT department for data extraction and sharing. This process limits access to and reuse of public sector data.

Finally, the assessment finds that the development of a government cloud infrastructure is a positive step toward secure data hosting and easier data access and sharing. However, the lack of a disaster recovery site is a major point of failure, and both a greater centralization of data in the government cloud and a greater use of data will increase the risks linked to the lack of such a recovery center. Similarly, the absence of a legal framework for data classification will slow and limit data migration to the government cloud.

The adoption of robust data governance frameworks and data management practices can have a transformative impact for the PA at different levels, as presented below.

- **Increasing data security:** The identification of data assets (inventories) will enable MDAs to identify and protect at-risk data systems that are playing an important role even though they not being documented or lack appropriate recovery and backup procedures.

- **Supporting the delivery of more e-services:** The identification of data assets, as well as the enactment of legislation, regulation, and policies that will ease their classification and their sharing, will enable MDAs to share and gain access to more data, thereby facilitating the design of more impactful e-services that will implement the “once-only” principle. These services will also ease MDAs’ work and increase their efficiency.

- **Increasing the efficiency of the public administration:** Access to and sharing of a greater volume of data between MDAs will enable them to mainstream data-driven decision-making, policy design, and monitoring and evaluation (M&E). These data-driven approaches enable MDAs to take better decisions and design more efficient programs in terms of impact and financial resources.

- **Supporting the development of the digital economy:** The identification and classification of data assets will enable MDAs to easily identify and proactively release data to the public. It will also enable MDAs to manage data requests more easily and quickly. A greater availability of public sector data will enable various categories of non-governmental actors (startups, innovators, academics, private sector, and the media) to build and deliver new and innovative data-driven services or analyses that could lead to the achievement of development goals.

In the longer-term, the implementation of the data governance framework will also enable the development and adoption of new data-intensive technologies such as artificial intelligence or data science.

Below are the key findings from the analysis of the public sector data governance in the WB&G. The last subsection provides an overview of the proposed action plan.

---

ACCESS TO INFORMATION

While ATI legislation does not exist, there is strong evidence that ATI is an important topic for civil society organizations (CSOs) and that there is a demand for ATI legislation to be adopted. A draft bill was produced by a coalition of CSOs in the WB&G and reviewed by international non-governmental organizations (NGOs); however, it has not yet been presented to the Prime Minister’s Office (PMO) and there appears to be no clear champion driving the legislative development process. There is significant interest from MDAs in adopting a unified and standardized set of data governance processes for public data release and in managing data requests more efficiently. Nonetheless, the absence of ATI legislation prevents MDAs from putting in place an efficient data request management procedure, leading to each MDA developing their own procedures in silos without alignment with others. MDAs are aware of the need for a standardized approach and have requested clear, harmonized instructions and procedures for implementation.

DATA CLASSIFICATION

The policies surrounding open data and statistics have clear provisions to support data classification. The Open Data Policy\(^3\) identifies the role of the Open Data Steering Committee (ODSC) to support ministries in data classification. Additionally, the statistics dissemination policy\(^4\) requires that statistical data be accessible to citizens. However, there is currently no standardized method for reviewing and classifying data given the lack of a government data classification policy, legislation, or directive. A key challenge is also the lack of a champion to drive the legislation development process. In the absence of unified and mandatory rules, each MDA has developed its own procedures, which are inconsistent across the board. The lack of data classification legislation or policy poses a challenge for a number of initiatives that MTIT is working on and that rely on data classification as an underlying enabler, including setting up a government cloud and the development of the Open Data Initiative. This issue was also underlined in recent assessments, such as the 2021 Cloud Readiness Assessment. Accordingly, there is a strong incentive to address this challenge and a tangible demand from MDAs for clear and harmonized guidance on how to classify their data assets. Work on data classification could serve as a foundational block and an enabler for ATI and the Open Data Initiative.

DATA MANAGEMENT

As the national statistics office, the PCBS has strong data management procedures in place that enable it to collect and publish robust national statistics in a timely manner. However, there is no policy or directive that guides or mandates a government data inventory. In most MDAs, data management is perceived merely as systems engineering or a database server responsibility, leaving the value of public sector data largely untapped in decision-making and service delivery. None of the MDAs met during the field visit have appointed designated data management staff to lead implementation of data management standards and processes in their entities. This is in part a reflection of broader human resources and technical capacity limitations across MDAs, where many entities appear to experience high staff turnover. That being said, MDAs continue to recognize the importance of a public sector data inventory for better data management and utilization and have shared demand for guidance and clear procedures to launch a data inventory process and implement data management good practice. This is an area for prioritization by the PA.

OPEN DATA

MTIT has massively invested in the development of the Palestine Open Data Initiative, which includes the execution of the Open Data Readiness Assessment, the establishment of a national open data

---


Executive Summary

The development of an open data policy that implements international good practices and establishes the ODSC and open data focal points in each MDA, and the organization of data training for MDAs. While having a strong policy and institutional framework in place is encouraging and a key foundational enabler, the next step in ensuring the maturity of open data ecosystems requires the WB&G to focus on improving access to, and usage of, open data. Currently, there are a limited number of datasets published (less than 40). The open data portal does not implement security requirements and has limited functionality. In addition, there is limited evidence of published data being reused by the public, owing to a lack of awareness of the existence of the open data portal and datasets available to end users, as well as issues with the relevance, quality, and reusability of datasets. That said, the opportunity to advance in this regard is promising given that MDAs are committed to the Open Data Initiative and have appointed OD focal points. One of the major challenges at the moment relates to the inability of MDAs, in the absence of an ATI or a data classification legislation, to identify data that could be openly released.

NATIONAL STATISTICAL SYSTEM

The national statistics office, the PCBS, is well regarded internationally with an overall rank of 20th out of 187 countries in the Open Data Watch Inventory 2020, and an overall SPI score of 70 out of 100 in 2019. The quality of data published by PCBS, its timeliness, and publication efforts (including use of various formats) are acknowledged by non-governmental stakeholders. The PCBS has adopted a range of policies to support data dissemination, support data reuse, and protect personal data while investing significantly in SDG data collection and dissemination, making data available publicly in various formats, including Excel. However, the remaining challenge is that the value of these national statistics is largely untapped in MDAs’ decision-making, policy design, and policy evaluation processes. This could be addressed by leveraging the vision PCBS set out for data stewardship in the Palestine Data Strategy 2022–2026 with the goal of realizing more value from data within the national statistical system and boosting the use of statistical data in evidence-based decision-making.

E-GOVERNMENT FRAMEWORK

Key underlying e-government frameworks have been implemented by the MTIT and used by a number of MDAs. This includes: (i) Zinnar, a robust data schema and ontology interoperability framework; (ii) X-Road/UXP, a secure data exchange layer for transactional operations; and (iii) Hukumati, the PA’s one-stop-shop portal for public e-services. This has created momentum within MDAs that see value in sharing data at the transactional level and in accessing other MDAs data, and that are eager to develop new e-services. At the time of this report, there is no prioritization strategy for e-services deployed on Hukumati. However, a service inventory and prioritization exercise is being implemented with support from the World Bank’s Digital West Bank and Gaza Project. The absence of implementation regulations in the e-transactions law is currently hindering the e-signature usage, which is a limiting factor for scaling up Hukumati. Moreover, municipalities cannot access and use the e-government framework because they are not considered to be government entities, leading to expensive duplication of infrastructure or inefficient data replication between the local and central levels of government. The extension and opening of the national e-government framework to municipalities would benefit them, MDAs, citizens, and businesses by reducing duplication, inefficiency, inconsistency from conflicting versions of data in different databases, and data risks related to cybercrime, cybersecurity, and personal data protection. The digitization of key shared registries, such as an address and a business register, will increase the

---

5 The open data portal is not using SSL encryption and, for example there are no interaction functionalities (with the exception of an email address) to ask for new datasets or ask questions or submit feedback on published datasets.

6 The main indicator that is currently used by the MTIT to monitor the portal and the Open Data Initiative is the number of published datasets.

7 Palestine country profile, ODIN report, https://odin.opendatawatch.com/Report/countryProfileUpdated/PSE/year=2020 Note that at the time of this report, the 2022 data for ODIN has been retired until July 2023 and the last official publication is the 2020 index.


value of the overall framework and enable the launch and delivery of new high impact services, such as G2B services.

**E-TRANSACTIONS**

Decree Law (15) of 2017 on the Electronic Transaction ("e-Transaction Law") provides an overarching regulatory framework for e-commerce/e-transactions. Though e-signature is recognized in the law, it is not used in practice due to the absence of implementation regulations. The Electronic Authorization and Electronic Signatures Unit, as stipulated in the law, has not been established. The delay in implementing e-signature has been flagged as one of the key barriers in scaling up Hukumati. In recognition of these challenges, the e-Transaction Law is currently being revised to make necessary amendments to enable a trusted and secure e-signature ecosystem to be put in place.

**PERSONAL DATA PROTECTION**

There is currently no personal data protection law of general application in the WB&G. That said, the Open Data Policy, cybercrime legislation, statistics law, and PCBS privacy policy\(^\text{10}\) include disparate provisions for personal data protection. The MTIT has been engaged in the process of drafting a bill for personal data protection and driving its adoption. The process is currently ongoing with a draft bill submitted to the PMO, and the bill is in the third reading by the PMO.\(^\text{11}\) At the working level, there is awareness regarding the importance of protecting personal data within different MDAs. In the absence of a national personal data protection legislation, each MDA is defining its own rules with little attempt to ensure consistency or alignment with each other. MDAs are, however, conscious of the challenge related to personal data protection, and they have expressed demand for a harmonized framework with clear guidance for classification and anonymization.

**DATA SECURITY**

The MTIT has set up a government data center to host critical government data systems. Data systems connected to X-Road/UXP are running on the government data center and are safely secured.\(^\text{12}\) Current information security policy defines a high-level framework to address data security, including backup procedures and physical protection measures, and the MDAs are responsible for adopting and adapting this policy to their needs. The MDAs appear to have good systems management practices. However, the current government data center has no disaster recovery site yet. Such a recovery site was being finalized at the time of this report outside the WB&G (Jordan). In the absence of a data inventory and given that each MDA maintains its own data infrastructure, legacy data systems\(^\text{13}\) may exist and be maintained by few people on obsolete hardware or software, putting their data at risk of being lost and causing critical disruption to national or international functions.

**RECOMMENDATIONS**

Based on the findings of the assessment, the study proposes an action plan with proposed interventions grouped into four main objectives to address the identified challenges and leverage strengths and opportunities.

- **Strengthen an enabling policy, legal, and regulatory environment** primarily on three main topics: (i) data classification; (ii) personal data protection; and (iii) ATI and data request

---


\(^{11}\) These have not been made available for review under this assessment, so it has not been possible to determine whether the law is expected to align with international good practice, including ensuring obligations for data controllers and fundamental rights of data holders, as well as the creation of an independent data protection authority.

\(^{12}\) Note that the assessment did not include any security audit to determine the level of security. The point here is that data on X-Road/UXP is centrally managed by the MTIT, which has more technical resources and expertise to mainstream international good practices.

\(^{13}\) The term "data systems" is used in the document to designate applications that host data such as information systems.
management. In the short term, it is necessary to provide a consistent framework for MDA compliance. In the medium/long term, it is important to ensure that corresponding legislation is in place, enforced, and implemented by each and every relevant MDA, including the development of implementation regulation for e-signatures to support the delivery of full online services through Hukumati.

- **Build data management capacity** to support MDAs in the implementation of robust data management processes. The proposed actions support building capacities of staff in data management, use, sharing, and publication, increasing the availability of technical resources, and putting in place an M&E plan to track the implementation by developing a fellowship program and training plans for data management skills for MDAs.

- **Implement technical enablers** that will support MDAs in their data sharing and data publication endeavor. In the short term, it is crucial to set up data inventories, design and adopt data management technical frameworks and data standards, and update the national open data portal. In the medium term, it is recommended to identify data systems at risk and secure them.

- **Strengthen collaboration and facilitate change management** to help MDAs increase data use in their activities to become more efficient and impactful and enhance the way they engage with their data users. In the short term, it is necessary to redefine and expand the mandate of the existing national open data coordinator (the MTIT) and open data coordinators within MDAs to create dedicated executive data manager positions that can oversee the overall data management processes. Also, it is important to take actions to develop use cases to demonstrate the power of data-driven decision-making processes and also to increase the demand for data. Medium- to long-term actions include a new internal organizational setup to facilitate the collaboration among MDAs and support greater use of data within society at large.

The proposed actions are summarized in a table in Annex I.
INTRODUCTION

Data serves many purposes in the public sector: first as infrastructure that supports services and enables transactions between diverse stakeholders in a network, from government to businesses and to citizens; and second as an evidence base for governance and decision-making. Data, when used effectively, are a powerful tool for governments in low- and middle-income countries to address their development challenges. For FCV countries, effective data usage could result in tangible outcomes that would mitigate specific challenges in different areas.

Most recently, the value of data was demonstrated through efforts to manage the COVID-19 pandemic using data to aid in disease contact tracing, provide information, guide policies, and inform spending of funds. In Morocco, for example, policymakers used data to develop various scenarios of the progression of the pandemic to shape lockdown and relief policies as well as inform where targeted efforts were needed to fund relief and recovery.

Public sector and government data sources such as censuses, national surveys, and administrative data, combined with data produced by the private sector helping to fill data gaps, provide timelier and finer-scale assessments of programs and policies, and serve public policy and development needs.

Businesses can create value from government data by integrating it with data produced by the private sector. When data are used as an input in production processes, they can spur innovation in products and services and reduce transaction costs, ultimately boosting productivity, growth, and opportunities, creating new markets, and supporting local entrepreneurship. This value added to the private sector as a result of a well-established national data ecosystem has the potential to create systemic and far-reaching economic growth.

This highlights the importance of efficient and effective data sharing, reuse, and interoperability between different actors (such as the public sector, businesses, and CSOs) to better realize development objectives. The enhanced use of data, however, also comes with new risks and concerns which must be addressed to ensure that the data-driven economy functions equitably and inspires trust within society.

Activities such as using public data for anticompetitive practices could lead to market concentration by large firms and lead to widening inequality and discrimination. Appropriate data governance frameworks, which include legal and regulatory safeguards, play a key role in protecting against these negative pathways and fostering trust, thereby expanding data value, use, and impact.

Realizing the opportunity that data presents for development requires that countries establish comprehensive data governance models to enable data production, use, reuse, and sharing. With such a data governance model in place, economic and social value is gained while ensuring that access to these benefits is equitable and that individuals and groups are safe from data misuse. For instance, while the earlier example of using Call Detail Records data helped countries to efficiently respond to the COVID pandemic, such data use also raises concerns for data protection. A reliable data governance environment that enables data sharing and use while also safeguarding personal data from being misused is critical for a sustainable data ecosystem. Trust is developed through multistakeholder engagement with individuals, civil society, academia, and the private sector.

The World Development Report 2021: Data for Better Lives describes data governance as being built on four key pillars: (i) data infrastructure policies, (ii) laws and regulations, (iii) economic policies, and (iv) institutions.

The enabling legal, regulatory, and policy framework for data is crucial for putting in place enablers and safeguards that foster trust in the data ecosystem. Creating such an environment involves adopting and effectively enforcing policies, laws, regulations, and technical standards to enable data to be used, reused, and shared while safeguarding the rights of parties to control their data or data about them and to ensure they are not misused or cause harm. Creating enablers for data sharing and interoperability through policies such as open data, ATI, open licensing, and technical standards for interoperability is a prerequisite for a data economy that benefits and sees accessible participation. Jordan, for example, supports government data accessibility by publishing specific datasets licensed under a Jordanian open government data license for anyone to use, reuse, and share their data.\footnote{16 World Bank. 2021. “World Development Report 2021: Data for Better Lives”. \url{https://www.worldbank.org/en/publication/wdr2021}.}

Data alone cannot solve these problems, however. People and diverse stakeholders are central to transforming data into useful information to provide better development outcomes. The inclusion of multiple stakeholders in a national data system encourages sustainability and helps ensure that all participants have an opportunity to contribute to the process and access and benefit from it.

Public sector data has enormous social and economic potential and is a founding pillar of the digital economy and digital transformation of a country. What it depends on is an appropriate governance framework that supports data standards, interoperability, accessibility, sharing, and reuse. The diagram below presents the components required to support efficient public sector data management and reuse.

A data inventory is a core component and the key first step of data management. Without information on what data an organization and its dependencies have, it is not possible for anyone to leverage the value of these assets. However, having a register of data assets is insufficient to support sharing. Data resources must be classified so as to define how to authenticate access and what redaction or modification is needed if it contains sensitive information (national security, personal data, etc.). Once an organization has an inventory and has classified its data, it can implement an easy-to-follow process to provide access based on a requester’s authentication status.

Even if accessing data from various public agencies becomes possible, the integration and use of these data further requires documentation that supports use of data and interoperability. Interoperability between parties to data sharing requires a description of the resource following standardized metadata definitions (ontologies, etc.). Finally, once one has appropriate data access rights and documentation defining use of the data, the next level is the physical act of accessing data. There are two ways to do so:
• **As transactional operations:** Data are accessed directly on a data system hosting it, and it is retrieved based on a query, on a per-record basis. For example, if there is an e-service that needs to retrieve the personal identity information of a user using an e-service, that e-service would query the population register to retrieve the information based on the unique personal identifier required.

• **As bulk raw data:** Data are accessed in the form of datasets containing rows reflecting multiple records. The bulk download could be available via an API or via a published extract from the hosting data system.

Transactional operations require a secure data exchange layer. Bulk raw data requires a data sharing portal (or open data portal for data shared under an open license). These data portals ensure that similar future data requests require no duplicated effort.\(^{17}\)

The report reflects the findings of a diagnosis of the policy, legal, and regulatory foundations underpinning a data governance framework, particularly for public sector data usage, in the WB&G that identify the existing elements and missing elements that prevent full implementation of the data governance framework as presented above. The study assessed the strengths and weaknesses of the existing legal, regulatory, and policy enablers and safeguards, identified the key stakeholders involved in public sector data generation, processing, sharing, and re-use, and proposes a roadmap of actions to address identified challenges to strengthen the data governance framework and to support the development of the data-driven digital economy in the WB&G.

This report describes the key findings on: **leadership** on data use and sharing in the government; key **enablers** for better public sector data use; key legal, regulatory, and policy **safeguards** that facilitate the trusted use, reuse, and sharing of data in a safe and secure manner; key **stakeholders** and their role and responsibilities in the data governance framework; and a proposed **action plan**.

\(^{17}\) Note that, depending on the source data, the data portal can provide access to data or access to the source API.
SCOPE OF THE ASSESSMENT

This assessment focuses primarily on the national level data governance framework and explores how different ministries and agencies manage, share, publish, and use data. However, as part of the field visit, the assessment also interviewed the Ramallah Municipality (RM) to evaluate the processes and data flows between different levels of governments and how the RM is leveraging data in delivering municipal services and decision-making. These investigations have uncovered interesting opportunities, activities, and challenges at the RM that are reported in the relevant sections of the document in the form of separate boxes. It is important to note that while these elements provide insights and highlight potential synergies with municipalities, the RM does not represent the extent of data use in other municipalities or reflect the current state of the Palestinian municipality setup in terms of technical, financial, and infrastructure resources.

LEADERSHIP

As a responsive government, the implementation of robust data management processes and the use of data for decision-making requires change management. From a data perspective, this includes legal, institutional, technological, and cultural changes, both inside and outside government. Focused, reliable, sustained political leadership is critical for a government so as to overcome resistance and inertia and incentivize stakeholders to make necessary changes in a timely and effective manner.

This chapter explores different elements of leadership. These range from political leadership and vision to development strategies and declarations by the leadership spanning the core dimension of digital transformation, such as data for decision-making, open governance, open data, e-government, and transparency.

DIGITAL TRANSFORMATION, DIGITAL ECONOMY, DIGITAL GOVERNMENT

The PA is a regional pioneer in digital transformation. E-government was adopted as a national priority in all its main policy documents and strategies in the early 2000s. The first strategic e-government plan was released in 2005. Since then, the importance of e-government and the role of the digital economy in Palestine’s social and economic development has been stressed in both national and sectoral strategies. For example, national policy 8 (“Improving Services to Citizens”) under Pillar 2 of the National Policy Agenda 2017–2022: Putting Citizens First (NPA 2017–2022) and the National Development Plan 2021–2023: Resilience, Disengagement, and Cluster Development toward Independence (NDP 2021–2023) includes the objective to “develop and implement an e-government strategy, focusing on the delivery of online services to citizens.”

The recent United Nations Development Program (UNDP)/E-Governance Academy Digital Maturity Assessment of the State of Palestine states that support for digital transformation is strong at the highest level of the government and at the top management of main ministries, and that there is consensus that the development of e-government and the digital economy represents an opportunity to address Palestine’s main social and economic development challenges. Finally, the

18 This section investigates the state of e-government in the WB&G from the leadership perspective, because an effective and efficient implementation of e-services and implementation of the “once-only” principle require data sharing between MDAs and an effective data governance framework. This section investigates only whether there is strong political and institutional support for the development of e-government services. Later sections dedicated to the e-government framework focus on the data sharing dimension of the e-government framework.
MTIT Information and Communication Technologies (ICT) strategy 2021–2023 includes the design and adoption of a digital transformation strategy and includes the expansion of the e-services offer with 68 new services.

### DATA AS A STRATEGIC ASSET?

Data does not seem to be considered as a strategic asset for governance by most MDAs, but rather as a technical responsibility under the ambit of their IT team. This analysis is based on the following evidence:

- There are no dedicated staff positions for data management.
- No MDA has established or maintained a data inventory.
- There are limited examples of data-driven policy making or decision-making processes.

However, there are examples of leveraging data for improved decision-making:

- The design and release of a COVID data service ([https://corona.ps](https://corona.ps)) helped the Ministry of Health (MoH) and the public during the pandemic.
- The geolocation and mapping of road traffic accidents by the RM in cooperation with police helped them identify dangerous intersections and reduce the number of accidents.

Following similar examples in every MDA should help them realize the potential of these approaches and put in place appropriate processes and organizational systems to leverage their development and use.

However, progress in implementing this e-government vision has been limited. Operational activities, such as defining specific targets and objectives, assessing required investment and engaging development partners in financing these activities, and setting up and closely following a robust M&E plan that will ensure that progress toward goals is measurable are currently missing. That said, it is important to note that there is a new whole-of-government e-government strategy being developed by the MTIT.

The PA officially launched an electronic government services portal—Hukumati—on January 8, 2023. As of January 2023, 1,100 new subscribers had signed up to the portal from the public, and 21 services were available on the portal. Hukumati relies on X-Road/UXP integration, and the combination of the various services has driven motivation toward facilitating the digital transformation in government services delivery. The process itself has become a driver of data sharing and interoperability in the PA. However, the study did not identify a strategy and processes to document all services within MDAs, evaluate the importance of the respective services, rank them in terms of impact, and select the ones that could be the most useful for citizens or the most impactful in terms of workload for MDAs, for example. Similarly, the study has not identified formal processes for feedback and response for those services currently being offered. That said, the MTIT is undertaking a service inventory of all citizen- and business-facing public services provided by MDAs in the WB&G to develop level 1 informational services and prioritize services for digitization. This exercise is currently ongoing under the World Bank-financed Digital WB&G Project.

One of the existing limiting factors for Hukumati is the lack of e-signature implementation because the e-transaction legislation is currently being revised to enable the use of digital signatures.

### DATA FOR DECISION-MAKING, OPEN DATA

Since 2018, there have been concerted interests at the highest level of the government in the release of open data. These efforts are followed by an Open Data Readiness Assessment in 2018, the establishment of a national open data committee by the Prime Minister, the adoption of an
open data policy by the committee, and the launch of an open data portal. The MTIT ICT strategy 2021–2023 also includes adoption of the Open Data Policy by the Council of Ministers (CoM). However, this political will and support has not yet translated into an active open data ecosystem. There is no open data strategy with clear goals or activities in place beyond a focus on the number of datasets published.

The MTIT ICT strategy 2021–2023 also includes the development of artificial intelligence (AI) through the adoption of an AI policy and the establishment of a council for AI. The MTIT has initiated work to develop frameworks for AI applications, code on AI ethics, use cases of AI in government services and socioeconomic development, and capacity building plans. However, these activities are preliminary steps, and while AI is presented as an major objective by MDAs, it appears too early for them to have clear plans or expected outputs. Nevertheless, AI development will increase the importance and demand for access and reuse of public sector data and will likely boost the Open Data Initiative.

Concerning the SDGs, the PCBS is responsible for collecting data to keep track of progress and monitoring. However, it has faced some challenges since certain data inputs are not part of its existing research surveys. It has implemented an additional process to assess each new survey to ensure that questions cover SDG requirements. However, unlike Mauritius (which has clear government leadership to rise to the top of the SDG rankings), Palestinian MDAs treat the SDGs as an adjunct to existing policy and do not appear to use it in driving policies or activities, even where leadership is aware of it.

OPEN GOVERNMENT, TRANSPARENCY, ACCOUNTABILITY

The National Vision stated in NPA 2017–2022/NDP 2021–2023 promotes open government, transparency, and accountability: “The Palestinian government is open, inclusive, transparent, and accountable. It is responsive to citizens’ needs, delivers basic services effectively, and creates an enabling environment for a thriving private sector.”

National policy 9, “Strengthening Accountability and Transparency,” in NPA 2017–2022/NDP 2021–2023 includes the objective to “strengthen transparency in government, including the approval and implementation of access to information legislation.” Currently, the draft ATI bill has not yet been passed in the WB&G. A draft ATI law was first prepared in 2005 by a CSO, Palestine Center for Development and Media Freedoms (MADA), and subsequently updated in 2012 with support from the Geneva Centre for the Democratic Control of Armed Forces, a Geneva-based think tank advocating for a good governance in the public sector. However, the draft ATI law was never presented to the PMO for formal review and approval. In the absence of ATI legislation, each ministry has developed its own ad hoc processes for data disclosure and access to public information independently of each other.

DATA SECURITY

The primary objective of the MTIT ICT strategy 2021–2023 is the creation of a national government data center and a disaster recovery center. This also includes design of a cybersecurity strategy, approval of an information security policy and its application (through a completed “comprehensive guide to information security procedures”), and the establishment of an Information Security Management System. The strategy is also supposed to include adoption of a backup policy and development of a backup procedure guide. The cybersecurity strategy is currently under development with the support from the United Nations Economic and Social Commission for West Asia (ESCWA) and not available yet.

---

22 The CoM has not yet adopted the open data policy.
PERSONAL DATA PROTECTION

The MTIT ICT strategy 2021–2023 includes the adoption of personal data protection legislation. However, there is currently no data protection law of general application governing the use, collection, and processing of personal data. A personal data protection bill was drafted by the MTIT and is in its third reading by the PMO. Most MDAs are aware of the sensitivity of personal data and have recently taken pragmatic measures to protect them. However, in the absence of a personal data protection act, each MDA has defined its own practices, and there is little consistency to the interpretation of data protection classification. For example, the Ministry of Interior (MoI) has technical experts for data anonymization and only shares aggregate data when the requested data contain personal information. The MoH protects patient information based on the Public Health Law of 2004, which is an important sectoral safeguard but not a replacement for a national data protection law. A data protection law of general application that is aligned with international good practice in terms of imposing limits on personal data processing and use, of protecting the fundamental rights of data holders, and of creating an independent enforcement authority, is a critical enabler to foster a “trust framework” around data use that supports usage of data-driven products and services, such as e-government services.

While MDAs are aware of the importance and sensitivity of personal data and their duty to protect it, they currently do not have tools, guidelines, or policies to help them operationalize that responsibility.

COORDINATION MECHANISMS

There are multiple institutional mechanisms within the PA that discuss and manage different dimensions relevant to the data governance ecosystem, such as e-government and e-services, open data, and the innovation and entrepreneurship ecosystem.

E-government has robust institutional arrangements in place:

• In 2014, the Higher Ministerial Committee chaired by the Prime Minister was set up to oversee the overall e-government strategy, coordinate and manage e-government budgets, integrate and redefine government policies and processes, endorse standards, and integrate schedules and plans. However, there is no evidence that this committee meets regularly or contributes to e-government strategy and implementation.

• The MTIT has the main responsibility for implementing e-government. There is a full department dedicated to e-government and an E-government General Coordinator has been appointed.

• Since 2010, the E-government Core Group (ECG) has been put in place. It is chaired by the MTIT and includes representatives from 19 ministries as well as representatives from academia (Palestine Polytechnic University) and the private sector (since 2016, with the Palestinian Information Technology Association of Companies). The ECG meets an ad hoc basis. Each ministry also has focal points responsible to the team. However, these are not full-time positions and their existing responsibilities do not allow them much time for an expanded workload.

Concerning open data, the ODSC was formed in November 2018, established by a Cabinet decision. It is chaired by the MTIT. However, it has no formal process for meetings or to agree on responsibilities. The Open Data Policy released in 2019 includes the designation of a national open data coordinator by the MTIT to coordinate all open data activities. The policy also includes the designation of open data coordinators at MDA level.

24 Originally, the ODSC had 11 ministerial members. It now has 18 members, including non-governmental actors.
The national open data coordinator was appointed by the MTIT along with a small team of 2–3 people. None work full-time on the open data project. The same goes for focal points in every MDA. Accordingly, while there is broad recognition and support for open data release, there is only limited capacity to deliver it and no agreed targets for what to deliver.

Since there is no ATI/data request process and no mechanism for data classification or consistent data protection, open data are seen and experienced as a separate class of data requiring additional resources and support rather than as a consequence or outcome of effective data management.

There is no formal mechanism for data requests and no formalized engagement with prospective non-governmental data users. The Palestinian territories are sufficiently small that informal methods for communication are in use, but this does not seem to result in greater data sharing.

Concerning statistics, General Statistics Law (4) for 2000 requires all ministries to create a statistics unit. These statistics units coordinate their work with the PCBS, and the PCBS has the authority to request data from the various ministries for the production of national statistics.

In March 2021 a “Technology and Public Administration” cluster was launched which aims to drive the digital transformation of the Palestinian government together with the private IT sector. The cluster is led by a steering committee, chaired by the Secretary General of the CoM, and includes the MTIT, the MoF, the Ministry of Entrepreneurship, the Ministry of Education (MoE), the Ministry of Higher Education (MoHE), the General Personnel Council, and the Palestinian Monetary Authority (PMA). This committee is mandated to “discuss and construct strategies for building and directing a Palestinian ecosystem to assist in developing the sector in all its technical, legal, human and financial aspects.”

Overall, “data governance” is seen as a largely technical problem and people tasked with responsibility for coordination and implementation (focal points, and up) are usually database and IT systems administrators. The broader “management” aspect of collaboration, coordination, integration, and contingency and continuity planning are not addressed.

**CONCLUSION**

Significant effort and initiative have been put into developing support and representation among MDAs to drive digital transformation within the government and its core elements: e-government services, open data, and digital entrepreneurship. The MTIT has created relevant coordination structures for each of the core topics, including representatives from non-governmental stakeholders. However, the lack of strategies with defined objectives and indicators for digital transformation or its sub-components, such as e-government or open data, and the lack of formal charter for coordination structures that do not meet regularly and lack specific agenda act as barriers for the effective and efficient implementation of the vision expressed in national strategies. In the same way, the absence of executive positions for data management within MDAs, together with a lack of clear guidance for specific conformance or delivery requirements, create siloed behaviors across topics and between MDAs.

---

ENABLERS: ENABLING DATA TRANSACTIONS/ FLOWS AND (RE)USE OF DATA

Public sector data, defined as data collected, produced, or controlled by public sector entities, can create development value when used effectively to improve the quality and inclusiveness of service delivery, increase accuracy in evidence-based policymaking, and promote government transparency and accountability through better ATI. Use, reuse, and sharing of public sector data, such as open government data, can also support innovation by enabling the development of data-driven insights, products, and services by non-government stakeholders. To enable these development objectives, this chapter identifies and assesses the underlying policy, legal/regulatory, and technical enablers that facilitate the use, reuse, and sharing of public sector data.

These include whether a government data classification policy and national interoperability framework exists, whether a policy framework for ATI and open data are in place, and whether government has both mandated and facilitated (for example, through standards and model terms) sharing of public sector data within and outside government. This section also includes investigations on the national statistics system and the role national statistics offices (NSOs) play in the data governance framework. Given the importance of official statistics as a source of public sector data for the data economy and the growing “data stewardship” role NSOs are starting to play in some countries in the broader data governance ecosystem, these investigations are critical to informing the assessment.

ACCESS TO INFORMATION

ATI “guarantees everyone the right of access to all information and documents related to the management of public affairs regardless of the status of the concerned person and the purpose for obtaining the required information.”

ATI supports data governance in two main ways:

1. Enforcement of the right to ATI is a means for anyone—including from within government—to request, access, and use public data from any public agency. In more recent legislation, ATI also includes provisions for proactive disclosure of information and data by public agencies.

2. ATI is dependent on a classification framework that provides guidance to MDAs on what can be publicly shared and what should be protected.

LEGAL & POLICY FRAMEWORK

Currently, ATI legislation does not exist in the WB&G. CSOs and coalitions, such as the Coalition for Accountability and Integrity (AMAN), continue to advocate for the right to ATI to be enshrined in law. In 2015 a group of CSOs held a series of consultative meetings at the invitation of the Palestinian Center for Development and Media Freedoms (MADA) with UNESCO support. The participant organizations were AMAN, the Media Development Center at Birzeit University, the Al-Haq Organization, and the Palestinian Journalists’ Syndicate. During these meetings, the latest updates concerning the draft law were discussed, including delays in passing it. These organizations agreed that a coalition would be formed called the “Coalition of the Right to Access to Information.”


28 In some jurisdictions, proactive disclosure of (open) government data is treated separately as part of a standalone open data law.

29 ATI legislation usually provides a classification framework that enables civil servants to determine whether information or a dataset can be disclosed to the public, proactively or on request. In some legislation, the ATI lists the set of information that can be released. In more comprehensive legislation, the open by default principle is established, with a list of exceptions. The aim of the legislation is to provide guidance to civil servants on determining whether any information can be disclosed to the public. Note, however, that a more detailed classification framework is also required to support data sharing within government. Such legislation is considered as an important enabler and is discussed in the data classification section.

A draft bill went through a series of versions analyzed by international NGOs but was never adopted. CSOs are still mobilized today on the topic and continued to advocate for such legislation. These activities were a follow-up on activities started in 2005 where AMAN-coordinated CSOs drafted an ATI bill in 2005. CSOs persuaded a government official to submit the draft to the Legislative Council in 2005, and the draft law was approved in a General Assembly debate on April 5, 2005. However, it did not complete all the necessary steps for enactment before the Legislative Council’s 2007 suspension.

Several other laws and policies provide some level of ATI. However, none of these provide a general right of ATI with mechanisms and scope that are aligned with international standards.

- **Press and Publication Law 9/1995**: The 1995 Press and Publication Law sets out the rules relating to licensing, ownership, and management of publishing enterprises, along with restrictions on the content of publications. The law includes a general right for citizens to access information from public bodies, requires public bodies to assist journalists and researchers, and defines material that cannot be published on the grounds of freedom, national responsibility, human rights, and respect of the truth and on content, including material harmful to national unity or which is inconsistent with morals.

- **Environment Law 7/1999**: The Environment Law aims to regulate pollution, protect public health, address environmental and biodiversity protection, and encourage the collection and publication of environment-related information. Under this law, any person “may also obtain any necessary official information to discover the environmental impact of any industrial, agricultural, construction, or other activity within the development programs, in compliance with the law.”

- **Public Statistics Law 4/2000**: The Public Statistics Law creates a statistics bureau to establish a unified and comprehensive statistics system for the Palestinian territories (Article 3). Under this law, all persons have “the right to obtain official statistics collected, processed, and disseminated by the Bureau in accordance with the adopted rules and instructions, taking into consideration the honoring of data confidentiality and individuals’ privacy.”

Laws and policies requiring proactive disclosure:

- **Law on the Regulation of the Public Budget 7/1998**: This law requires ministries to provide budgetary-related information to the Public Budget Directorate. It requires this body to disseminate the public budget to the media and public following Palestinian Legislative Council approval. It also requires the Ministry of Finance (MoF) to prepare and the minister to present to the Cabinet and Parliament quarterly reports assessing compliance with the budget, including significant deviations. The law further requires ministers to publish their decrees regarding terms of loans and transaction guarantees in the official gazette.

- **Law on the Finance and Administrative Oversight Bureau 15/2004**: This law gives the Finance and Administrative Oversight Bureau the authority to view all reports, data, and information held by the civil service and reports of investigations into financial and administrative law violations. It also allows the bureau to request, access, and preserve any information from public bodies, including information the public body deems confidential. The bureau chair is required to submit quarterly and annual reports to the president, Cabinet, and Parliament on its activities, findings, and observations. Nothing in the law requires the bureau to publish information.

- **Law for the Election of Local Councils 10/2005**: This law requires the Central Elections Commission to publish the voter rolls and names of lists and candidates in each district and polling station.

---

• **Elections Law 9/2005**: This law requires district offices to publish their voter rolls and the Central Election Commission to publish the list of candidates for president. Final results should be published in the official gazette and daily local newspapers.

• **Anti-Corruption (Amended) Law 1/2005**: Under this law, the Anti-Corruption Agency has the power to collect information related to corruption, to create a database and information systems on corruption cases, and to coordinate with the media in creating a culture of integrity and anti-corruption.

• **Open Data Policy**: The ODSC has formulated an open data policy which aims to support government commitments contained in the agenda of national policies and plans, sectoral strategy, best practices, and SDGs. It aims to boost government performance, increase its efficiency, expand coordination between government agencies and other sectors, improve government services, and foster economic development. From the perspective of ATI, there are a few important elements that are included, such as proactive disclosure, data publication under Creative Commons Attribution (CC-BY), and reuse for commercial, non-commercial, and journalism purposes.

• **PCBS policy for proactive dissemination**: This policy requires the PCBS to engage in the proactive dissemination of statistics.

• **PCBS dissemination policy**: The dissemination policy (latest version September 2019) defines the PCBS’s dissemination activities.

The draft ATI law was never presented to the PMO for formal review and approval. The two main challenges hampering the process appear to be the lack of a government champion to drive adoption and the government’s general reluctance to rely on a CSO-drafted bill.

**INSTITUTIONAL SETUP**

There is no legal basis for ATI and, therefore, no centralized independent body to process ATI requests. All requests are dealt with by their respective departments under the various legal provisions mentioned above. There is no focal point for data requests, which currently must go to the minister or permanent secretary instead.

**CAPACITIES**

International evaluations were conducted in 2013/2014 by the Center for Law and Democracy on the various drafts of the bill with recommendations given on best practices. UNESCO also organized meetings to promote and engage with the government and the Ministry of Media (MoM) in particular. Excluding these, no other activities on capacity building were identified. In the absence of legislation, ministries interpret processes independently and without alignment between them.

The interviews with MDAs indicated a clear demand for guidance on policy, methodology, and implementation for ATI and data requests to ensure consistency and conformity. They also described the challenges and constraints they face in implementing these processes on their own.

---

33 [https://www.pcbs.gov.ps/Portals/_Rainbow/Documents/Proactive-Dissemination.pdf](https://www.pcbs.gov.ps/Portals/_Rainbow/Documents/Proactive-Dissemination.pdf)

DATA REQUEST PROCESS

MDAs manage a labor-intensive process for governmental and non-governmental data requests (including bulk source data) which requires initial validation from a minister, agreement and signing of an MoU, and its implementation by an IT team. Each MoU is implemented separately and re-executed whenever the requesting body needs changes or new data.

This approach is ad hoc and inefficient:

- It can take multiple weeks to complete the MoU process.
- It adds a significant workload to already under-resourced IT teams.

The lack of a dedicated process to process and implement requests means that it is difficult to ensure efficiency.

A data inventory and classification of all data assets would permit rapid triage of requests and the automation of a process to proactively produce data for all parties with appropriate rights to access it, limiting the need for a formal data request process to all but the most sensitive data.

As a natural consequence, all public data could be automatically published to the open data portal, populating it with useful datasets, and creating momentum for data reuse.

IMPLEMENTATION PRACTICES

AMAN is the CSO coalition to promote ATI, as mentioned above, and remains active in its advocacy role. There is no evidence of any corresponding activity by government over the last few years. It also seems that the evolution of the draft in the 2013/2014 was not positive, with new drafts weakening the previous one (see analysis).

This process is stalled with little prospect of progressing as a legislative decree. Alternative approaches are required and requested by MDAs.

In terms of data request management, each MDA operates in the same way, although the outcome at which they arrive may be interpreted very differently from each other.

In the absence of a formal data access and request process, the current mechanism is that any request for access to unshared data must start with a letter of motivation sent to the minister of the relevant ministry. This applies to both intergovernmental and private/third-party requests.

The minister decides whether to allocate the request for further evaluation. Once (or if) approved, an MoU is signed and a focal point assigned for data release.

There is no register of decision-making and no mechanism for documenting this process (that is, an informal classification register does not exist). Since there are no shared public data inventories, many of these requests are purely speculative to find out whether the data exists. Given the delays and complexity, ministries querying data from each other may simply duplicate data to save time. For instance, field investigations show that such duplication occurs with geospatial data. In the same way, non-governmental stakeholders experience significant difficulties accessing government data, and often withdraw their requests after weeks of delays. This process results in the negotiation and management of many MoUs across government and leads to excessive duplication and wasted resources in MDAs already struggling with capacity and budgetary constraints.

CONCLUSION

There is strong evidence that ATI is an important topic for CSOs, and they have been organizing active advocacy activities for more than 15 years. At the government level, recurring interest has existed since 2005, with different draft bills released at different periods but without clear sustained activities or interest.

The lack of a clear champion to drive the adoption process and interact with the PMO, along with the general reluctance to rely on a draft bill developed by civil society, results in the absence of noticeable progress with the draft bill not even being presented to the PMO.

However, there is a significant interest by MDAs in adopting a unified and standardized set of data governance processes for public data release and to manage data requests more efficiently.

It is important to note that different policies in different sectors (open data, statistics) require proactive disclosure of data. For statistics, MDAs must release corresponding data, the boundaries of the policy are clear (national statistics), and the access to and reuse of national statistics is well defined. Concerning the Open Data Policy, the scope and boundaries of datasets covered by the policy are defined in general terms and enable MDAs to largely interpret the applicability of the policy. Moreover, since the Open Data Policy is not an official law, implementation is not mandatory but rather adopted on a voluntary basis by MDAs.

For non-governmental data users, bulk raw data are of most use. For data which are at the intersection of the public and private (such as a business register or simply a list of licensed restaurants), the PCBS is not the appropriate vehicle for publication and release. Its legislated mandate specifically precludes it from openly releasing any raw data, with the exception of subsets of anonymized microdata provided in the form of public use files.

The Open Data Policy itself does not provide a comprehensive set of mechanisms for classifying data for release. It is, effectively, only “open” or “closed,” with no guidance on data protection or redaction for release. As such, the Open Data Policy in and of itself is really only useful for supporting publication once data have been openly classified, but not before. The development of the Open Data Initiative will therefore require a legal framework for data classification through ATI and/or data classification legislation.

DATA CLASSIFICATION

Data classification relates to laws, policies, and regulations that enable any public institution to evaluate the sensitivity of data assets and the practices that need to be associated with each level of sensitivity (for example, the ability to be stored on a private cloud, the ability to be shared widely within the government or with non-governmental actors, required accreditation to access and use the assets).

LEGAL & POLICY FRAMEWORK

There is currently no government data classification policy, legislation, or directive. West Bank and Gaza: Digital Policy Dialogue Cloud Readiness Assessment (World Bank: 2021) provided a recommendation for developing a data classification methodology, assessing what class of data is suitable for public cloud versus private cloud. The assessment also states that a data classification exercise is necessary to measure the level of confidentiality and sensitivity of government data to optimize usage. The MTIT ICT strategy 2021–2023 does not include an activity to produce such legislation, although data classification remains a prerequisite for efficient government cloud implementation and for easier data publication and data request management processes.
The Open Data Policy\textsuperscript{36} identifies the role of the ODSC to support ministries in data classification. The policy establishes that all data published on the open data portal are open and reusable following CC-BY 4.0 license requirements. It describes classes of data that cannot be made public (personal data, data protected by intellectual or commercial rights, security data, and data that may compromise national security or national interests). The policy allows datasets to be published after removal or anonymization of data that are subject to these exceptions.

The statistics dissemination policy\textsuperscript{37} requires that statistical data be open and reusable under a CC-BY license.\textsuperscript{38} The Law on the Regulation of the Public Budget 7/1998 requires ministries to provide budgetary-related information to the Public Budget Directorate, which must disseminate the public budget to the media and public, subject to Palestinian Legislative Council approval.

Finally, the information security policy\textsuperscript{39} mentions the concept of “classified information” which refers to “categories of information that have been classified according to security regulations.” The policy considers two levels of classification (classified and highly classified) with different constraints, such as the need to encrypt the higher level of classification before sending it over a network. In the same way, classified information should be transmitted via email using an authorized system. Except as mentioned above, there is no information about the evaluation of classification in the policy. This policy does not provide actionable indications on how to classify information and is therefore insufficient to support data classification.

Most MDAs interviewed recognize that the lack of data classification is a major challenge for them in terms of data sharing and data publication. There is strong demand for government-wide guidance to ensure consistency and conformity between existing heterogeneous processes.

**CAPACITIES**

There is no evidence of any program related to capacity building on data classification. There are also no agreed-upon guidance or processes which could inform such capacity building.

**IMPLEMENTATION PRACTICES**

There is no evidence of any classification activity beyond that conducted for publication on the open data portal. Any requests for information are sent to the relevant minister who decides as to whether it will be considered. Once it is passed to an appropriate manager, a decision about release will be made, subject to an MoU. There is no formal classification, but only an ad hoc decision-making process based on individual requests.

**CONCLUSION**

The lack of data classification legislation or regulation/policies that are mandatory across the government represents a major gap in the Palestinian legal framework, which negatively impacts several areas, from cloud computing to open data. That said, some classes of data, particularly open data and statistics, have a clear classification in their respective policies and have an identified reuse license. However, there is no standardized method for reviewing and classifying data as part of a management process. This has knock-on effects in contingency and staff/system continuity planning, and across the data governance and management of key databases.

While, in the absence of preliminary work or a draft and the lack of a champion to drive the adoption process, the passing of a full data classification act will require a relatively long time, a government-
wide policy proposing a standardized approach for data classification would significantly help MDAs in managing data requests and in their data management processes. Given the interest and needs expressed during interviews, there is a clear demand for such guidance that could be adopted on a voluntary basis. In the absence of both an ATI legislation and a data classification legislation, it would be appropriate to focus on the development of policy frameworks for data classification as an enabler for ATI and for the Open Data Initiative.

OPEN DATA

Open data means that "anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)." The objectives of an open data initiative are to leverage and facilitate, from both a legal and technical perspective, the sharing and reuse of public government data inside and outside government.

LEGAL & POLICY FRAMEWORK

An open data policy was adopted in 2019. However, in the absence of an ATI legal framework or any other related legislation about proactive disclosure, the scope of the policy and the data that are covered by the policy cannot be clearly established. The policy is applicable to the entire public sector, requiring the appointment of a national open data coordinator who will work with the national ODSC to create a register of open data for release and to collaborate with specific publishing agencies to ensure data are placed on the open data portal. The policy calls for proactive disclosure and alignment with the Open Data Charter principles. The policy assigns the coordination of open data to the MTIT.

The policy has been prepared, adopted, and released by the ODSC (which has the mandate to do so), but has not been approved yet by the CoM. At this stage, policy implementation is not mandatory, and MDAs adopt it on a voluntary basis.

Data for publication are to be licensed under Creative Commons Attribution. The policy recognizes the need to protect and exclude different categories of data such as personal data, data protected by intellectual or commercial rights, or national security data, but there are no regulatory barriers to reuse for any purpose. Reuse permits commercial, research, and journalistic use. The policy derives its non-revocability from its Creative Commons license. It also mentions free (no-fee) access to data. The policy charges the ODSC with managing and advising on data classification.

The policy includes a minimal technical framework that imposes:

- The publication of datasets that meet at least a three stars on Tim Berners-Lee five-star scale.
- The publication of raw data.
- The completeness of data.
- The use of open format and, in particular, CSV file format is recommended as the preferred option, followed by XML or JSON and then SHP or GeoJSON. Compressed formats (.zip, .rar) are forbidden except in exceptional cases (large file, no other options).

Note:

40 http://opendefinition.org
41 In this section and in the context of open data and statistics, the term "data sharing" means the sharing of raw bulk data in the form of datasets.
43 Open data principles define how public government data should be published to maximize its potential impact. However, the identification of government data that can be made public depends on ATI legislation.
45 https://opendatacharter.net/principles/.
46 CC-BY 4.0, https://creativecommons.org/licenses/by/4.0/. The license is cited and referenced in the policy and therefore all its terms apply, including non-revocability.
• The publication of datasets in a “timely” manner, without further definition on constraints on data update.

• The use of Arabic for Arabic datasets, and Arabic and English for datasets in two languages. It also imposes the use of English for descriptive metadata.

The policy includes a detailed nine-step publication process starting with identifying data for release, up to correcting errors and updating the dataset (defined in generic terms). However, the instructions are high-level and do not provide technical or standard guidelines for publication. The policy also establishes direct access to data without a requirement for user authorization or authentication. It further obliges data owners at public agencies to correct any errors, omissions, or lack of clarity as soon as it is identified.

There is no policy obligation to manage publication requests or provide responses to requests. There is an email address on the open data portal but there is no public guidance on what will happen following any request via the portal—it is unclear who will respond, or what form that response will take.

Finally, the policy defines priorities in dataset publication: development sectors (education, health, agriculture, economy, population, transportation, and data used in scientific research), government services (such as the distribution of various service centers), data infrastructure (such as information systems), geographic and demographic data, and data for which there is high demand or expected high demand by users.

The main challenge is that publication commitments are voluntary. The policy, as it stands, provides a mechanism for publication (with protections for publishers and users) but no requirement or prescription on what must be published. In the absence of a data inventory, without a clear understanding of the concepts of open data, and without ATI legislation or data classification legislation, MDAs are not able to identify data that should be published under the policy, nor they are able to identify and experience benefits for such effort.

Currently, while the ODSC has a mandate over data which is published, it has no mandate to suggest what data should be published or to monitor and compel publication and updates. The team itself is composed of 2–3 people, of whom one responds to requests via the website. However, as described previously, data requests must comply with the current MoU process, and each MoU is defined on its own terms and scope. Requesting via the open data portal does not side step the requirement for the requester to apply in writing to the minister concerned. The ODSC may be able to help identify whether the data exists and which ministry to request it from, but cannot go any further. Note, though, that there is no data register, so the ODSC has no specific knowledge about what data are available either and thus needs to ask MDAs directly. This is time-consuming and the lack of resources can affect responsiveness. Currently, there are very few requests as the site is not easily discoverable or widely used.

Given this general lack of mandated publication, the ODSC has few tools to compel data standards or disaggregation to point data. This is still ad hoc and voluntary, and no ministries have started processes to release and update such point data. Finally, the open data policy does not include any performance indicators or an M&E plan. The main criterion that the MTIT uses is the number of datasets published. This indicator does not reflect the quality of the data published, its usefulness for potential reusers, or the processes in place at MDAs for publication.

The PCBS uses SDMX for statistical data and metadata exchange and Dublin Core for descriptive metadata. Technically, this means there is institutional knowledge about using metadata standards,
and the PCBS can add this to existing capacity building training, but in practice MDAs’ main and only experience with data standards is limited to Zinnar\textsuperscript{51} compliance for X-Road/UXP.

**INSTITUTIONAL SETUP**

Responsibility for delivering and coordinating the Open Data Initiative resides with the MTIT, which appointed a national open data coordinator responsible for managing the service and developing collaboration with publishing agencies. There is also a national ODSC which is responsible for deciding on whether data qualify for release. Finally, the policy creates the requirements for government agencies to appoint open data coordinators. Given technical (IT) and financial challenges at municipality level,\textsuperscript{52} it is unclear how data requests would be communicated to local authority level or what the regulatory mechanism would permit such request and release given their legal definition as non-government entities.

In terms of coordination with non-governmental stakeholders, the policy establishes general principles and charges the ODSC with communicating with media, academic, investment, and entrepreneurial institutions to promote open data and organize training. The ODSC also includes representatives from non-government actors.

All ministries have an open data focal point, but this is usually someone in the IT team with a full-time role as systems engineer or database administrator. It is a purely technical position, and they are not responsible for driving the open data agenda within their organization, deciding on what will be released, or how that release process is to be implemented and updated. They also lack a holistic understanding of the variety of data that exists within the ministry.

The ODSC can provide support if it is requested, but there is no formal process of meetings or agreeing to responsibilities or a diary of releases and updates. Since there are no formal meetings, NGOs have little capacity to guide release and no legal mechanisms—aside from the MoU process—to request release.

Based on the investigation with the RM, municipal/local government data requests seem to work in the same way as those for MDAs but, since local government is not officially considered as a government entity, it is not included in the responsibilities of the ODSC. This means that local government release does not fall under the ODSC mandate, and the ODSC has no framework to work with it proactively. This includes access to and use of the open data portal.

**CAPACITIES**

The policy assigns the responsibility of organizing training sessions and capacity building sessions for the ODSC. These sessions are expected to cover both public and non-governmental agencies. The ODSC also has a mission to raise awareness on open data. The policy invites public institutions to coordinate and collaborate with non-governmental agencies. The strategic plans have significant training objectives, but it is not clear how many people were trained or what their expected learning objectives were.

The MTIT has run eight open data courses since 2018. The MTIT provides supporting letters for graduates to take to their managers, but the overall outcome of these sessions is limited, with only 39 datasets currently available on the open data portal.

Interviews with NGOs indicate that public awareness of the Open Data Initiative is low. Of the seven organizations present, only half had heard of the open data portal. Those who are aware and have investigated it reported that the data published is in aggregated form, usually old, and therefore not useful for their needs. The two main data users described their need for point, and not aggregate,

\textsuperscript{51} Zinnar is the interoperability framework set by the MTIT to leverage transactional data exchange between ministries on top of UXP/X-Road.

data to deliver their services. They also found it difficult to find the site since it is not indexed by Google (because it is not served over SSL).

While the non-governmental ICT sector has not found use in open data, ministries themselves are committed to the project with focal points and intentions to release. However, as mentioned earlier, open data focal points are IT professionals without a clear view of data available at the ministry level (lack of data inventory), without the right to release data, and without information on the needs of reusers.

During the interviews, it seemed that while MDAs are generally unaware of open data benefits or how to implement the Open Data Policy, they are interested in the topic and would like clearer guidance and support to engage effectively and efficiently in the Open Data Initiative. In particular, they understand the potential value of data inventories and are eager to set them up with appropriate guidance.

**IMPLEMENTATION PRACTICES**

The open data portal was launched in November 2021. There are 20 ministries registered as publishers and 10 have produced datasets. It is not discoverable on a public search engine (Google, for example) and is also not specifically on a PA domain (gov.ps). This is likely a result of not providing necessary SSL security certificates to serve the website over https. The portal is based on the CKAN package, an open-source data management system.

It was unreachable during part of the desk research and does not seem to be considered as a critical government service. Portal security is limited with no use of SSL, for example. In terms of functionality, there is no module for managing dataset requests (except an email address) or managing comments on datasets.

In terms of content, datasets have limited metadata, such as short descriptions, few keywords, and automatic metadata generated by the portal (date of upload, last data of modification). Most datasets seem to provide metadata in both English and Arabic.

There are 39 datasets available on the portal. The MTIT's plan is to reach 250 datasets published in 2023. They all have the policy-recommended license CC-BY 4.0 and are in CSV. However, a random evaluation of the datasets shows that many datasets, even if published recently, either have no date or refer to data from before 2014 or even before 2000.

![Figure 1. Palestine Open Data Portal (source: www.opendata.ps)](image)

---

53 This assertion related to sectoral MDAs interviewed during the field visit. It is not the case for the MTIT and the PCBS, which are perfectly aware of open data benefits and have strong data management practices.
55 [https://ckan.org/](https://ckan.org/).
Critically, no geospatial data are available on the portal. There is a dedicated geoportal called GeoMOLG, but the website is unreachable outside of the WB&G and, during office hours, requires an approved login for use.

There is no evidence of the existence of a data inventory which would guide users as to what data are produced by government agencies, no indication of how data were selected or prioritized for release, and no update process defined for datasets (individually or generally). While there are social media links, these are the generic components included in CKAN, and there is no broader approach to promoting public engagement on reuse or sharing case studies.

There is no evidence of any activities relating to data reuse, communication activities with non-governmental actors, or innovation activities relating to data published on the open data portal. However, the MTIT ICT strategy 2021–2023 includes the organization of innovation contests.

In terms of content, data selected are ad hoc without real engagement with civil society or commercial data users. This is due largely to the capacity, time constraints, and information of the open data focal points combined with the Open Data Policy being stranded from a more general data management process and policy (ATI, classification, data protection).

This cascades through to portal development. There are no plans to invest further in the system, and any request management process must wait on broader ATI, classification, and data protection initiatives.

Since local government is not included in the initiative, any open data effort is at their own initiative. The RM has extensive open data release on their municipal portal, including a dedicated GIS service. This is an outlier as most other municipalities and local authorities have no such initiatives.

One additional piece of open data is in the public accessibility of tenders and contracts. Here, the Palestinian territories are in conformance with international transparency trends and these are available, but with the common lack of integration between local and national government.

CONCLUSION

Since 2018, the MTIT and the PA have invested in the development of the Palestine Open Data Initiative. There is a clear intention to maintain international best practices in the development of the initiative by putting in place a dedicated steering committee, with non-governmental representation and a national open data coordinator, and adopting an open data policy which also follows international good practices. The portal itself is based on the CKAN package, which enforces publishing standards. Despite this foundation, there is little project momentum and no evidence of engagement for data reuse. Data published on the portal are limited (with only 39 datasets), not highly visible, and are both out of date and of limited interest for data reusers, be they CSOs, private companies, or academia. The lack of momentum is due to several factors, such as the fact that the policy is not mandatory (thus limiting its effect and its implementation by MDAs), the lack of clear guidance and methodology for MDAs on different topics such as data publication, data classification, or personal data protection, the absence of data inventories to identify candidate datasets, and the lack of interaction with potential data reusers to understand their needs.

56 [https://geomolg.ps/](https://geomolg.ps/)
58 [https://palopenmaps.org/view/3229/@31.90431983,35.19614924](https://palopenmaps.org/view/3229/@31.90431983,35.19614924)
NATIONAL STATISTICAL SYSTEM

National statistics, including SDG-related data, are an important source of public sector data for the digital economy. In the same way, the NSO is usually a major player in the data ecosystem as regards defining the technical framework for data format and exchanges and reference data.

LEGAL & POLICY FRAMEWORK

The Palestinian General Statistics Law 4 of 2000\(^\text{59}\) provides the legal basis for the collection, processing, and use of statistical data. The law establishes regulatory frameworks for the PCBS as an independent NSO responsible for providing statistical data to inform government and the public, including a data stewardship role across government.

While the law does not go into the technical requirements for how to prevent inadvertent disclosure, it does require the statistics bureau to ensure that personal and individual or commercial financial data is kept confidential and that specific data (for example, via the national census) can never be used to pursue criminal cases against anyone. The only legal basis for using any data, including tax data, collected by the statistics bureau in a criminal case is to investigate contravention of the law itself. The summary of these points is accessible and public on the PCBS website in English and Arabic.\(^\text{60}\)

The statistics law is complemented by a dissemination policy\(^\text{61}\) and a proactive dissemination policy.\(^\text{62}\) The dissemination policy includes guidance on accessibility, openness, relevance, quality and coordination, independence, trust, confidentiality, coherence of release across multiple channels, and techniques (including requirements for visualizations and international standards). The policy includes the adoption of the Creative Commons CC-BY license for statistics. The proactive dissemination policy is limited and only states that the PCBS must release statistics based on the statistical calendar after validation and that all users may access the statistics at the same time.

There is a right to reuse individual data where the individual has specifically approved such use as part of a survey microdata release. All microdata that are classified as available for sharing with authorized researchers is served on the PCBS National Data Archive (NADA) portal.\(^\text{63}\) This is an open-source data publication platform developed with support from the World Bank to support research distribution of International Household Survey data and is an industry standard. The PCBS has a review team to assess personal data protection issues and prepare data accordingly (either via specific redaction, aggregation, or classification as non-releasable).

There are approximately 330 English surveys and 323 Arabic surveys on NADA.\(^\text{64}\) Researchers can register and request access after agreeing to the terms of use from the user. The application is assessed and, if access is agreed, the user can download the microdata. Researchers are not permitted to republish the data, but must cite PCBS as a data source should they publish a paper (they are not required to publish).

In addition, the PCBS will produce custom aggregation slices of its statistical data in response to queries. If there is agreement that these datasets can be republished, then it will be under CC-BY.

In total, it receives about 2,000 requests for microdata and custom statistical series annually. It does not charge for these services.

\(^\text{63}\) NADA Data Catalog, [https://nada-ihsn.org/](https://nada-ihsn.org/).
INSTITUTIONAL SETUP

The PCBS was established in 1993 and is responsible for producing and disseminating national statistics. It is a functionally independent unit of government in terms of its regulatory mandate to act as an impartial and independent state body.

The statistics law also requires each ministry to set up a statistical unit. The PCBS coordinates all these units. The roles of the unit are:

• To enhance coordination between the PCBS and the ministry.

• To make use of data available in the field of its ministry’s scope of work and prepare such data for dissemination or for use by the PCBS or the ministry.

• To maximize the potential for launching crucial functions inside the ministry, such as planning, studies, and research.

• To work with the PCBS on ensuring the proper data flow from the ministry to the PCBS.

• To enable the PCBS to consider the ministry’s statistical needs.

PCBS data are mainly based on census and household survey data, but it is trying to improve its use of the ministry’s transactional data for statistical series. This requires it to agree on MoUs with each MDA and train statistical units in each of them to support their data requirements. Its objective is to build a solid national system of statistical data based on actual/operational data from the ministries. Its challenge is the inconsistent capacity within ministries.

GEOSPATIAL DATA

Geospatial data suffers from atomization. The Ministry of Local Governorate (MoLG) is responsible for maintaining the GeoMOLG portal, which should contain all enrichment data layers that add geospatial point and boundary data to maps (census boundaries, addresses, flooding, roads, etc.). However, according to some MDAs, the MoLG seems to lack capacity and resources to ensure this service is up to date, and updating layers takes time.

As one of the most regular users of geospatial data for producing statistical series, the PCBS does its best to provide data to MoLG for updating, but runs its own parallel internal geospatial service for its own purposes. Other MDAs also consider GeoMOLG insufficiently consistent for professional use, triggering a proliferation of subsites that are largely unreachable (and unknown) to other MDAs.

However, the situation will likely improve soon. Good Shepherd Engineering, a geospatial company supporting the Palestinian government, is collaborating with the Palestinian Land Authority (which manages cadastral data) to improve coordination between MDAs for geospatial layers maintenance.

The PCBS was involved in the development of the Zinnar schemas and is trying to motivate ministries to standardize their definitions on this even where their data are not uploaded to the X-Road/UXP data sharing platform. The PCBS cannot use X-Road/UXP for its aggregations because the system is purely for transactional operations. It needs all the data or aggregations based on all the data.

While MDAs report using data in decision-making, there is no evidence of how well the PCBS-produced resources are used to guide policy or formulate a response. The study could not identify documents (policies, reports, etc.) that refer to national statistics to present analysis, make decisions, or engage in activities.
CAPACITIES

The PCBS provides continuous and regular training activities across government to promote understanding, technical capacity, and the use of government statistics in decision-making. However, progress has been limited, with many departments still producing and using their own data independent of the PCBS. The learning objectives for these training sessions are not clear, and training material is not publicly available. The main challenge for the PCBS is insufficient capacity within the MDAs. Ordinarily, there are only two to three people in each ministry available to dedicate time to PCBS responsibilities.

The PCBS is also engaged with the Arab American University of Palestine in the Data Science Initiative. This initiative has ambitious goals to train interested people from the public and private sector, universities, unemployed people, and international organizations working in the Palestinian territories as well as associations to raise awareness on the importance of data science in governance for leaders. This data science training program will be added to their slate of capacity building programs for the ministries. Development is still a highly provisional and not yet fully absorbed by ministry leadership.

The PCBS’s main priorities in training relate to gaining expertise in R language through a full training program comprising nine skills. Digitization of paper-based systems is a critical objective over the next three years so that the PCBS can ensure a greater opportunity to research transactional data.

IMPLEMENTATION PRACTICES

The PCBS is well regarded internationally with an overall rank of 20th out of 187 countries in the Open Data Watch Inventory 2020, and an overall SPI score of 70 out of 100 in 2019. The PCBS has also invested massively in SDG data collection and dissemination, making data available publicly in various formats, including Excel.

The PCBS website is kept up to date and includes very recent data. The existing policies are clearly listed on the PCBS portal. Data on the portal are presented as HTML tables and downloadable as Excel XLS (that is, proprietary) format. Under the dissemination policy, all data are released under the same Creative Commons license as the open data portal. Data are disaggregated by governorate and gender, with a complete register of all available data.

The performance of the PCBS is clearly acknowledged by non-governmental stakeholders, who underline the improvement of the bureau and easy access to national statistics.

CONCLUSION

The PCBS appears to be a well-respected NSO, performing well on international indexes. In addition to founding statistics legislation, several policies promote the proactive dissemination of statistics and the reuse of data. It also publishes data on a dedicated website. Via the data science initiative, it works on developing capacity within broader society for data analytics. However, while non-governmental stakeholders are pleased with their access to national statistics, the value of national statistics is largely untapped in MDAs’ decision-making, policy design, and policy evaluation. For instance, the study did not identify any policy or document that reference national statistics as a rationale for decision-making, proposed actions, or activities.

68 Palestine country profile, ODIN report, https://odin.opendatawatch.com/Report/countryProfileUpdated/PSE?year=2020. Note that the 2020 data for ODIN are the last available data at the time of this report. The 2022 data were published in February 2023 and then retired in March 2023 until July 2023.
E-GOVERNMENT FRAMEWORK\textsuperscript{72}

The term “e-government” relates to the application of ICT to government functions and procedures to boost efficiency, transparency, and citizen participation. The objective of an e-government framework is to work toward making all government services (government to government – G2G; government to citizen – G2C; and government to businesses – G2B) available online. The development of a robust e-government framework requires data exchange/sharing between MDAs, which requires data interoperability, and an integrated exchange across all MDAs—national and local—to maximally benefit from the efficiency and accessibility gains which come from a shared, “once-only” approach to data provision.

E-GOVERNMENT INFRASTRUCTURE AND SETUP IN WB&G

The MTIT has been working on e-government services since the early 2000s. Since then, different initiatives and platforms have been implemented. As of today, the delivery of public e-services in the WB&G relies on an architecture that includes three major building blocks:

1. **A secure data exchange layer:** The MTIT has adopted Estonia’s X-Road data exchange platform, recently renamed UXP. This platform allows MDAs to share their information and data systems at a granular level (deciding who has access to which set of information) and enables other MDAs to query and access these data in real time and perform transactional operations through a standardized interface and set of protocols. There are now about 1,400 services on X-Road/UXP from 53 ministries. The authentication process for X-Road/UXP is decentralized. In practice each ministry has a sign-on access point, but individual sign-ons are managed by the MDA directly. A user is granted access to the X-Road/UXP server within their ministry, and then a generic MDA-level access request is logged on X-Road/UXP. This has resulted in different implementations of the sign-on process at different ministries. Based on what their ministry permits, users then have access from the 1,400 services available.

2. **An interoperability framework:** The MTIT has led the design and adoption of Zinnar, the formal register of schema and ontology definitions. Zinnar is used to describe any data definitions and support schema-to-schema interoperability. X-Road/UXP is dependent on Zinnar for its utility. Zinnar can go dormant for long periods if no new data systems are intended to be added to X-Road/UXP.

3. **A one stop-shop e-services portal:** The MTIT internally launched a centralized e-services portal, Hukumati,\textsuperscript{74} in August 2022 with access extended to the public in January 2023. There are initially 21 services from 9 MDAs:
   - Passport application status
   - Driving license renewal
   - COVID-19 test results
   - Land registration query (koshan)
   - Property tax payment by property details
   - Driving license practical test results
   - Status of a land or apartment transaction

\textsuperscript{72} Note that the e-government framework is investigated mainly from the data sharing perspective. For example, Hukumati, the one stop-shop for citizen and business e-services, is explored from the perspective of the implementation of the once-only principle, and the exchange of data between MDAs, not as a tool for improving service delivery.

\textsuperscript{73} In the context of e-government and in this section, the term “data sharing” means the sharing of data at the transactional level (that is, the ability to query a data system at a given MDA to get a record associated with someone or a business).

\textsuperscript{74} Hukumati, This Week in Palestine, August 2022, \url{https://thisweekinpalestine.com/hukumati/}. 
• Clearance certificate for property tax for transfer ownership purposes
• Certificate of non-conviction record
• Taxpayer number
• Financial purposes clearance certificate
• Status of address change request
• Theoretical test results (driving license)
• Health insurance fees
• Property tax payment through taxpayer number
• Newborn registration
• Apartment registration report (koshan)
• Property purchase application status
• Work permits within the ‘48 borders
• Payment of traffic violations
• Clearance certificate for property tax for municipal purposes

The MTIT has developed a single sign-on (SSO) procedure for Hukumati, with citizens’ SSO registration managed by the MoI. Citizens register on Hukumati and then visit their closest MoI office to validate their subscription with their official papers and get their accounts validated.

Hukumati depends on the success of Zinnar and X-Road/UXP and allows citizens to access and interact with services that rely on their own personal data available on the X-Road/UXP platform.

The diagram below illustrates the place and role of each building block.

---

E-GOVERNMENT AT MUNICIPALITIES

Official policy defines municipalities as outside the government, excluding them from X-Road/UXP and Hukumati. The consequence is infrastructure duplication and challenges for citizens.

The RM has no access to the population register to validate individual identities to provide their services, and so manage its own database. It also keeps its own address and business registries.

During COVID-19, the RM established an e-services portal to avoid office visits. This proved successful and it now charges higher fees for in-person services. Its e-portal parallels Hukumati, leading to the proliferation of the complexity it was meant to avoid.

The RM is an obvious outlier. Few municipalities have resources to implement such a system, but municipalities still maintain costly parallel systems, including paper-based systems, to deliver their responsibilities.

Integration of municipalities into the national data governance framework would resolve these challenges.

---

An e-government infrastructure also usually includes a series of shared reference data registers used by all MDAs. This component is largely unspecified within the PA. There are no officially adopted government-wide data registers, and, therefore, some data systems shared on X-Road/UXP serve as de facto data registers. The best example and the most used and useful data register is the MoI-managed population register (including the registration of births and deaths, and the delivery of electronic birth and death certificates). There are others, such as the vehicles register, which are de facto data registers managed and maintained by the MDA in which it is based, sometimes with legislation that describes it (for example, population register) but often without any related legislation. Sometimes there are specific shared processes for updating the register (for example, a dedicated system for hospitals to register births and deaths with the MoI) and sometimes not (for example, registering a vehicle requires a visit to a Ministry of Transport office). This can sometimes result in complex registrations. A business owner must first visit the Ministry of National Economy to get a recent, hand-signed business registration certificate, then take that to register their company vehicle at the Ministry of Transport. Citizen-to-government data exchange seems to be improving, but business-to-government exchange is still largely paper-based and atomized, due largely to the lack of a common shared businesses register. The business register is a focus of the PCBS Data Strategy 2022–2026, indicating that it may still only be in development, although other MDAs, like the Ministry of National Economy, also develop their own business registries. In the same way, there is no address register, thus making the physical delivery of documents extremely challenging. The lack of core data registers or duplicated registers impedes progress and creates challenges for MDAs in the design of specific services or in their ability to map their data systems with other MDAs. Finally, the lack of e-signature usage in practice (see section on e-transactions) is a limitation for scaling up Hukumati. There is no way today for any MDA to deliver official papers online, and services that aim to deliver such official papers require citizens to physically visit a government office after completing the process online. There is no apparent formal process or deadlines to address this shortcoming. Of the 21 Hukumati services, 6 are for obtaining an official document.

Despite these limitations, the setup of the e-government infrastructure with shared interfaces, processes, and standardized access, along with a standardized way to design and put in place e-services, has created momentum within MDAs. Based on the interviews conducted during the field visit, most ministries are planning to design, build, and release Hukumati services, although there is a distinct gap as to where municipalities would also be. The RM has its own set of online services, but they are excluded from Hukumati, thus creating multiple e-services entry points for citizens. One Hukumati service is specifically dedicated to bridging this gap, permitting users to download a property tax clearance certificate to present to their municipality. Were municipalities on X-Road/UXP, this step could be automated within government without the need for citizen intervention.

LEGAL & POLICY FRAMEWORK

There is no dedicated legislation or policies related to a Palestinian e-government framework, but a number of relevant provisions are in Decree Law (15) of 2017 on electronic transactions, which is investigated in the next section dedicated to e-transactions. However, an e-government strategy is currently being drafted and finalized by the MTIT.

There is a Cabinet decision that stipulates X-Road/UXP as the only option for data sharing between MDAs. There is no other legislation or policy related to the use of Zinnar or Hukumati. As such, there is no legal framework on the use of data registers such as the population register.

---

76 There are no policies or regulations that establish specific common government-wide data registers.
These gaps in the legal and policy framework for e-government have been underlined in several recent studies from the World Bank, UNDP, and the PCBS and MTIT themselves. At the time of this report, there are strategies underway for the development of e-government services and for the digital transformation of government. However, the MTIT ICT strategy 2021–2023 includes the development and adoption of a digital transformation strategy and the adoption of a roadmap for the e-government strategy, and this is a work in progress.

**INSTITUTIONAL SETUP**

The MTIT is responsible for e-government delivery with a department dedicated to e-government and an appointed e-government general coordinator. The MTIT is well regarded as a leader in providing technical infrastructure underpinning e-services for other agencies. The challenge is that MDAs tend to work on their own as best they can, fighting for visibility, budget, and resources within a severely constrained environment.

The ECG has been in place since 2010. It is chaired by the MTIT and includes representatives from 19 ministries, academia (Palestine Polytechnic University), and the private sector (since 2016, with the Palestinian Information Technology Association of Companies). The ECG is largely an assemblage of MDAs with an interest in e-government and expands in proportion to this interest, with individual MDAs managing their representation. There is no formal requirement for regular meetings, a specific agenda, or any specific/measurable objectives. The ECG meets on an ad hoc basis at the request of its members and has limited follow-up and reporting responsibilities. Lacking proactive and structured engagement, MDAs only call on support from the MTIT when they need it and on an ad hoc basis. This leaves the MTIT to respond reactively with no coordinated role or responsibility.

In 2014, a Higher Ministerial Committee, chaired by the Prime Minister, was formulated to oversee overall e-government strategy, coordinating and managing e-government budgets, integrating and redefining government policies and processes, endorsing standards, and integrating schedules and plans. This committee also meets on an ad hoc basis.

There is a National Interoperability Committee to manage the development and update of Zinnar. However, this committee and the work on Zinnar can lay dormant for long periods if no new data systems are intended to be added to X-Road/UXP. The committee was reestablished in February 2020 through a Cabinet decision.

Hukumati is a cross-government initiative where the MoF is responsible for the portal business/operational model and the MTIT leads technical aspects. It is developed entirely internally at the MTIT by a dedicated team. After some months testing the sign-up process with ministry staff and civil servants, the system itself went live for public registrations in early January 2023. A communication/marketing strategy is still being developed.

Since e-government and data interoperability are largely seen as technical—rather than policy or management—challenges, focal points are based in the systems engineering or database management teams with many other responsibilities. It is not unusual for a systems engineer or IT manager to be a focal point for multiple MDAs, spanning multiple responsibilities, including MoUs for data sharing. Moreover, in the absence of a data governance structure within MDAs and of an executive-level data management position, MDAs have major difficulties in gaining a holistic view of their data assets.

---

81 Resolution 9 in [http://www.palestineCabinet.gov.ps/portal/Decree/DetailsEn/26110818-aa5a-4721-8c92-c7c5584b433f](http://www.palestineCabinet.gov.ps/portal/Decree/DetailsEn/26110818-aa5a-4721-8c92-c7c5584b433f).
Given the general lack of resource or budget and the ad hoc nature of the process, there is limited opportunity for MDA-to-MDA coordination or experience-sharing on how to design services or address challenges, for example.

CAPACITIES

The MTIT received support from the Estonian E-Governance Academy\(^\text{82}\) to set up and operate X-Road/UXP. In terms of capacity building initiatives, two activities were launched:

- The setup of the Palestinian e-GOVERnance academy (PalGOV), funded in 2010 by the EU to develop capacity in e-government issues. Content was developed by both the MTIT and academic partners (Birzeit University).
- The ICT training center, launched in 2014 and funded by the Korean International Cooperation Agency, with the mission to develop and deliver training programs for government officials and staff in e-government matters.

The PalGOV appears to no longer exist.

The e-payments team meets weekly, but most teams meet every one to three months. There is no formal record of these meetings, but they are recorded at the PMO.

Capacity building is based on surveys of need and MTIT assessments. However, topics are specialized and do not cover general data management processes and practices.

The PCBS and MTIT are setting up a national school to coordinate all e-government, data, and statistical training for the public administration but the budget for this initiative has not yet been agreed on. The MTIT is trying to motivate for essential data/data infrastructure for government, including e-services, in the hope this would drive support from the ministries. There is currently a tender being developed to promote integrated open data training and capacity development, but the budget has yet to be approved.

The MTIT is currently working with ESCWA to draft the Palestine Digital Agenda 2030, which includes training and capacity development.

CONCLUSION

With X-Road/UXP and Zinnar, the e-government infrastructure appears to be a successful factor for designing and launching e-services. MDAs have clear guidance on how to access and share data at transactional level, and access to the population register appears to be of great value for all MDAs. Access to more registries, such as the businesses or address registries, would further increase the value of this infrastructure. The recent launch of Hukumati has built up MDA momentum to invest in e-service development and promoted greater use of UXP. All MDAs have developed plans to increase the number of services they will offer to citizens.

\(^{82}\) https://ega.ee/

DATA AT RISK

Data systems connected to X-Road/UXP are documented and maintained via the government cloud. Conversely, existing legacy data systems are known to only a few people (some close to retirement) and poorly documented, and many are running on obsolete or proprietary software.

These data are at enormous risk.

As an example, the antiquities management system in the Ministry of Tourism and Antiquities (MoTA) is one example. The software is similar to Microsoft Access, with the database stored on MoTA servers. It was developed by its current manager 20 years ago and details about 40,000 antiquities identified in Palestine, encompassing all its documented cultural history. Data are shared with researchers on request around the world.

While there is interest in sharing more generally, the proprietary software requires that requests must be made to the one single person who manages and who also built and maintains it, and that he responds directly.
A limiting factor is the lack of e-signature support, requiring people to physically visit government offices to get official documents. Currently, e-services are citizen-focused services (G2C). The lack of a unified business register prevents the development and delivery of businesses e-services (G2B), which should be the focus of the next stage of the development of e-services.

**E-TRANSACTIIONS**

Laws governing e-commerce and e-transactions provide an overarching legal framework that helps create trust in both public and private sector data transactions online, which in turn encourages use of data online. A best-practice regulatory environment for e-transactions begins with establishing legal equivalence between paper-based and electronic communications, that is, ensuring that a digital data transaction will not be denied legal value simply because it is performed electronically and ensuring that electronic evidence has probative value. For example, establishing legal equivalence for electronic contracts and signatures requires equal legal status as hand-written ones.

Additionally, e-commerce/e-transactions laws are needed to govern the way in which parties to an online transaction are authenticated. Most laws governing e-transactions take a layered approach to digital authentication of parties to a transaction, with built-in recognition that certain types of online transactions require greater degrees of certainty about the identity of parties, while others require lower levels of assurance. Other trust services may also be specified as a basis for verifying and validating e-signatures, seals, or time stamps; verifying and validating certificates to be used for website authentication; and a range of activities related to data transfers.

An important tool for authentication of parties to a digital transaction is a trusted foundational digital identification system, with widespread coverage (designed to ensure inclusiveness and non-discrimination), permitting individuals to securely prove their uniqueness to authenticate themselves in online transactions. Foundational digital identification systems can be an important enabler for individuals to access public and private sector services online.

**LEGAL & POLICY FRAMEWORK**

The relevant legislation for e-transactions is Decree Law (15) of 2017 on electronic transactions enacted on July 9, 2017. This legislation also covers e-signatures. Managed by the MTIT, this law grants legal equivalence between paper-based and electronic communications, with some exceptions:

- Transactions involving a change in personal status: marriage, divorce, wills.
- Transactions involving the sale or rental of real estate.

These are common exceptions aligned with the UNCITRAL Model Law.\(^3\) The legal equivalence covers contracts, signatures, and any correspondence.

This law appears to provide for the creation of a hierarchical public key infrastructure (PKI) model where a dedicated unit within the MTIT is set up to manage authentication and e-signatures, with a mandate to put in place an authentication and signature service. Pursuant to the law, this unit should serve as the official certificate authority (root certifier responsible for issuing certificates) for all public institutions and public entities. Under this function, the law requires the MTIT to identify mechanisms, the duration of, and the conditions for the preservation of electronic data, along with audit certificate providers, which are activities that require a significant amount of specialized technical capacity (and raises questions of liability if the integrity of the certificates issued is breached). The MTIT unit, as the certification authority, also has a mandate to license external parties to conduct similar services. This approach is quite prescriptive and puts a significant amount of legal and technical responsibility on the MTIT. A more flexible regime would limit the MTIT (or another

\(^3\) [https://uncitral.un.org/en/texts/ecommerce#:~:text=The%20most%20widely%20enacted%20text,principles%20of%20non%20discrimination%20against.](https://uncitral.un.org/en/texts/ecommerce#:~:text=The%20most%20widely%20enacted%20text,principles%20of%20non%20discrimination%20against.)
entity acting as the certificate authority) to playing a regulatory function and issuing licenses to third parties to certify the validity of electronic communications. While this may raise the costs of certificates being issued, this issue would stabilize with sufficient competition in the market for providers.

The legislation authorizes all public entities to manage all transactions in electronic format, provided that appropriate procedures and policies have been adopted. Documents are considered valid if they include a valid e-signature authenticated by the certificate authority and if they are themselves validated by the certificate authority.

E-signatures are valid and officially recognized only if they are registered within an authentication service. The implication of these provisions is to require a stricter assurance level (only achievable with digital signatures that enable the authentication of the individual’s identity) and stringent requirements to guarantee the technical reliability of electronic communications, such as for the preservation of the mechanisms used to issue the e-signatures. Foreign digital signatures are recognized only if they have been issued by an approved entity, even if the overall process for recognizing a certificate authority is underspecified in the law\textsuperscript{84} and there are no implementing regulations associated with the legislation. Together, these provisions may not meet the principles of technology neutrality and non-discrimination enshrined in the Model Laws on E-commerce and E-signature, which recommend that e-signatures be regarded as meeting legal requirements provided that the methods used are "as reliable as was appropriate for the purpose."\textsuperscript{85}

Though the functional equivalence between electronic and wet ink signatures is recognized in the law, fostering digital signatures and PKI with the current structure of the implementation arrangements poses a significant challenge for implementation. The lack of implementing regulations that would clarify certain provisions, such as procedural requirements for the validation of e-signatures, is an additional limitation. The implementation gap is evidenced by the fact that the Electronic Authorization and Electronic Signatures Unit, as stipulated in the law, has not been set up. Moreover, given the legal reliance on PKI in the e-transactions law, the absence of complementary enablers, such as a reliable foundational digital identification system which could be used to support reliable authentication, has a compounding effect. These have been identified as key barriers in scaling up the e-government service portal, Hukumati.

In recognition of these challenges, the e-Transaction Law is currently being reviewed as part of the World Bank Digital West Bank and Gaza Project to support the establishment of a trusted and secure e-signature ecosystem. The law will be revised on the basis of a legal gap analysis to make necessary amendments to enable the use of e-signatures in accessing services in a way that ensures the functional equivalence between paper-based and electronic communications, non-discrimination, and the technology neutrality of the means of securely authenticating e-signatures. The appropriateness of the institutional arrangements and implementation regime for issuing certificates will also be considered as part of the broader legal review, taking into account existing implementation challenges.

No legislation has been identified concerning a digital identification platform. However, the population register maintained by the MoI is a core register shared on X-Road/UXP and is used by all MDAs that need identity verification. In September 2020, the MoH and MoI, with support from UNDP, launched a digital births and deaths registration system.\textsuperscript{86} On registration of a birth, Palestinians receive the identity number used across all government services, including education and healthcare. Almost all live births are registered since medical care is provided by clinics and hospitals rather than by midwives or general practitioners. Deaths, however, are less likely to be

\textsuperscript{84} For example, the law appears to make a substantive distinction between “accreditation” (Article 40) and “recognition” (Article 42), raising questions about the interoperability and overlaps between these different regimes (based on ex ante versus ex post mutual recognition).


registered, especially in rural areas or smaller villages. These systems have not been evaluated for alignment with good practice,\textsuperscript{87} as this is beyond the scope of this assessment.

\textbf{INSTITUTIONAL SETUP}

The 2017 e-Transactions Law empowers the MTIT to oversee the implementation of core infrastructure, such as the certificate authority. The MTIT ICT strategy 2021–2023 includes launching an authentication and e-signatures unit (certificate authority), but the unit has not been set up yet.

\textbf{CAPACITIES}

There is no evidence that the e-transaction law is being implemented within public institutions, especially as regards electronic document authentication and digital signatures, as the Electronic Authorization and Electronic Signatures Unit has not been set up in the MTIT.

\textbf{IMPLEMENTATION PRACTICES}

E-signature and e-document authentication are not yet in place. In general, each MDA says they have no objection to e-signatures but are waiting for the unit in charge to be set up and for practices to change globally within the government after the amended law is passed.

\textbf{CONCLUSION}

While the 2017 e-Transactions Law defines a generic framework with the potential to fully support transactional e-services—including e-signature and legal equivalence of electronic documents—it has not been implemented, and there is no e-signature or authentication service. The MTIT is working toward resolving this challenge with updated e-transaction legislation, but there is no timeframe for implementation.

\textsuperscript{87} For example, with reference to the Principles on Identification for Sustainable Development (available at: https://www.idprinciples.org/), notably principles on inclusiveness and non-discrimination and data protection by design and default.
SAFEGUARDS: TRUST IN DATA FLOWS AND THE (RE)USE OF DATA

This section focuses on legal requirements that protect fundamental rights in personal/mixed/sensitive data. Issues covered include data protection and cybersecurity/cybercrime.

PERSONAL DATA PROTECTION

The fundamental rights individuals have regarding their data are protected to enable their agency and control over the data that they produce or through which they can be identified, so that these data are not misused, such as for targeting, surveillance, or discrimination. These rights are substantive (including the right to control how data are collected, used, and disclosed to or shared with third parties) and procedural (including ensuring data are used in a transparent, proportionate, and accountable way, and that those who suffer a data breach are notified and can be compensated through meaningful redress mechanisms). These rights are usually mirrored with obligations imposed on parties who control the data being collected, processed, or used to ensure these rights are respected.

The first step in creating a robust national legal framework for data protection is for governments to adopt a comprehensive data protection law that meets best-practice criteria while adapting to the local context. The law may be adopted as a standalone or as part of omnibus legislation. Countries that have not adopted a data protection law of general application may have sector-specific rules for personal data protection (for example, health or banking data), but these protections will be limited to the sector.

LEGAL & POLICY FRAMEWORK

The Palestinian Basic Law serves as the constitutional framework for the Palestinian legal system. It criminalizes “any violation of any personal freedom, of the sanctity of the private life of human beings, or of any of the rights or liberties.” According to the law, “every attack on any of the personal freedoms or the sanctity of the private life of the human being and other rights and public freedoms guaranteed by the Basic Law or the law, is a crime in which neither criminal nor civil lawsuits are subject to statute of limitations, and the National Authority guarantees a fair compensation for those who have been harmed.” It also guarantees Palestinian citizens access to fair remedy if their fundamental rights are violated.

In practice, however, there is no ratified data protection law. The PA has prioritized the adoption of the cybercrime law (Law 16/2017), which was enacted in 2017 by presidential decree (see Cybersecurity section). This cybercrime law was then amended (Law 10 of 2018) to address some of the concerns Palestinian legal experts and civil society had raised. This law does not touch on personal data protection except in Article 22, which prohibits “arbitrary or illegal interference with the privacy of any person or the affairs of his family, home or correspondence.” This article also prohibits “publishing news, photos, audio or video recordings, whether live or recorded, related to illegal interference in the private or family life of individuals even if they are correct.”

However, the law also potentially conflicts with key data protection provisions, such as data minimization and transparency obligations. It obligates internet service providers to retain users’ data for at least three years and to provide the public prosecutor access to all data and information when needed. It also grants the public prosecutor the authority to order the immediate collection of unrestricted data, including monitoring private communications, traffic data, and metadata.

In 2019, the Palestinian CoM in Ramallah issued Resolution (3) of 2019 regarding the protection of personal data of Palestinian citizens. This resolution applies only to the use of personal data for commercial purposes and prohibits such use before obtaining prior permission from the owner of the personal data. It does not apply to public institutions.

Personal data protection is also mentioned in the Open Data Policy and in the statistics law and PCBS privacy policy. The policy clearly states that personal data must be protected, and datasets with personal data cannot be published without redacting these data. The statistics law has several articles (4, 16, 17, 18) that protect personal data. The law also includes a right to reuse individual data where the individual has specifically approved such use, and penalties for breach of limits on the processing of personal data. The PCBS has adopted a privacy policy that reinforces personal data protection in surveys and censuses. The policy also covers information collected on the PCBS website.

The lack of a comprehensive and holistic personal data protection legislation has been underlined as a critical gap in the legal context of the Palestinian territories for data governance, and the MTIT ICT strategy 2021–2023 includes the design of such legislation (Privacy Data Protection Act). The drafting process has already started, and the bill is in its third revision after comments from the PMO. However, there is no timeline set for adoption and implementation.

Despite the absence of a regulatory policy, MDAs are aware of the sensitivity and importance of protecting personal data. However, each MDA is interpreting and implementing this in their own way. This can sometimes have impact on existing processes. For example, the PCBS described how they used to get access to the MoI-managed register of births and deaths without removal of personal data, but that (after the data were linked to X-Road/UXP, and the MoI received training on data protection) they resolved to no longer share raw individual data and rather conduct aggregations themselves. The PCBS has had to work with the MoI to guide it in producing the aggregations they need for national statistics.

In the absence of policy, methods, or definitions, each ministry interprets as best they it can—and with the intention of ensuring data protection—but with what can be users very inconsistent results for their potential data. MDAs are aware of this inconsistency challenge and would like harmonized guidance and policy that will provide a government-wide framework. However, there is no established timeline for the adoption of the current draft of the legislation, and its implementation (establishment of a data protection authority (DPA)) may take several years.

**INSTITUTIONAL SETUP**

There is no institutional framework, such as a DPA or its equivalent, responsible for receiving complaints or ensuring redress. There is no evidence that complaints are received or managed.

**CAPACITIES**

While there is no DPA, there is evidence of capacity and awareness among MDAs, and particularly at the PCBS which clearly states that no personal information will be shared, and any personal information will be treated as confidential. The main challenge is related to consistency in measures taken to protect personal data across MDAs. On the technical side, apart from the PCBS, which advises some MDAs on how to anonymize statistical data, anonymization capacity seems limited to redaction techniques.

IMPLEMENTATION PRACTICES

Despite the lack of legislation or a DPA, MDAs engaged during the field visit were all concerned with the need for personal data protection. The PCBS is a clear champion in this area and provides a privacy protection disclaimer, guaranteeing the anonymization of personal and personally identifiable data in all the surveys they manage. These protections are stated on its website and in a dedicated policy. However, there is no consistency in terms of protection measures or technical anonymization across MDAs.

CONCLUSION

The lack of generally applicable personal data protection legislation is a major challenge for safeguarding the publication and sharing of data. Despite some protection provisions inserted in various policies, such as the Open Data Policy and PCBS policies on privacy and dissemination, the overall lack of legislation, of clear definitions for personal data protection, and of an independent authority to manage and protect personal data is problematic.

Despite MDAs being aware of the need to protect personal data, their processes and approaches are heterogeneous. However, they are conscious of this challenge and want a harmonized framework with clear guidance for classification and anonymization. While the adoption and the implementation of the current draft legislation will take time, the design and release of a voluntary framework which applies to all MDAs should be a first step to resolving the current challenge, and act as an interim measure until the full act is adopted and implemented.

DATA SECURITY

A key element in establishing trust in a data ecosystem for personal and non-personal data is ensuring security of network infrastructure and elements over which data flow. This section explores infrastructure, policies, and regulations that relate to data security.

LEGAL & POLICY FRAMEWORK

The first cybercrime and cybersecurity law was adopted in 2017 by Law by Decree 16 of 2017 on cybercrime.\footnote{https://security-legislation.ps/en/law/100111#text=a%20specialised%20cybercrime%20unit%20shall%20be%20attached%20to%20the%20ministry%20of%20justice%20and%20jurisdiction.} This legislation was then replaced under pressure from civil society by a new law adopted in 2018 (Law by Decree 10 of 2018 on cybercrime).\footnote{https://security-legislation.ps/sites/default/files/law/Law%20by%20Decree%20No.%2010%20of%202018%20on%20Cybercrime.pdf.} This law was then amended in 2020\footnote{https://security-legislation.ps/en/law/100198.} to redefine Article 15 to increase the penalties defined in this article. Supported by ESCWA, the MTIT is also currently working on the development of its national cybersecurity strategy.

Aside from the cybercrime law, the MTIT has adopted a data and information security policy\footnote{https://www.mtit.gov.ps/phocadownload/policies/security.pdf.} that was approved by a Cabinet decision (Cabinet Decision 09-122-18/2021- Data and Information security policy). In general terms, this policy requires public institutions to ensure the confidentiality, integrity, and availability of information systems, including those managed by external parties.

It requires physical protection of computer rooms (from an access, but also environmental, perspective). It also requires public institutions to adopt, publish, and implement an IT security policy and document and test emergency and disaster response plans for critical information systems (but with no information about what a critical information system is).

The policy includes recommendations on the storage of backup media containing essential or sensitive information (without a clear definition of essential or sensitive information) to be at a safe distance from the main site. However, there is no requirement on backups themselves, except that
backup and recovery mechanisms should be documented, periodically checked, and implemented regularly.

The policy also has a section on data access that requires owners of the relevant information to provide access authorization based on user needs. Authorization must be regularly reviewed. The policy further requires public institutions to conduct audits and security risk assessments on information systems and applications every two years.

There is no specific clause related to personal data in the cybercrime law except in Article 22, which prohibits “arbitrary or illegal interference with the privacy of any person or the affairs of his family, home or correspondence.” This article also prohibits “publishing news, photos, audio or video recordings, whether live or recorded, related to illegal interference in the private or family life of individuals even if they are correct.” There is no mention of personal data protection in the information security policy or of the need to protect systems that host personal data and provide access on a need-to-know basis.

The cybercrime law stipulates that “State agencies, institutions, entities and the bodies and companies affiliated therewith shall abide by the following:

1. Take preventive security measures needed to protect their own information systems, electronic websites, information networks and electronic data and information.

2. Promptly notify the competent authority of any crime provided for under the Law by Decree as soon as it is detected or when uncovering any attempt of unlawful reception, interception, or wiretapping, and provide the competent authority with all relevant information to divulge the truth.

3. Keep information technology data and the subscriber’s information for a period of not less than 120 days and provide the competent authority with such data.

4. Cooperate with the competent authority to implement their powers.”

The law establishes a cybercrime unit within the police agencies and security forces to investigate cybercrimes. A CERT team within the MTIT has been set up and is running.96

INSTITUTIONAL SETUP

The MTIT organized a survey on cybersecurity practices within government institutions at least once in 2018 (Readiness Assessment Survey in Cybersecurity for Government Organizations in Palestine).97 This survey does not thoroughly investigate security measures in place related to data protection (backup, personal data protection, etc.). Unfortunately, the data related to this survey are not accessible for security reasons.

Recently, a new Cabinet resolution created a national cybersecurity agency, which will be responsible for implementing relevant policies. Once it is operationalized, the Palestinian Computer Emergency Response Centre (PalCERT) will be housed within the agency.

CAPACITIES

For security reasons, this information was not shared with the team.

95 The cybercrime unit established by the law within the police agency and security forces.
96 https://cert.ps/.
**IMPLEMENTATION PRACTICES**

There is evidence⁹⁸ that the MTIT has put in place a government data center the aim of which is to store up to 20 percent of total government information. While the capacity of this data center is limited, the MTIT is developing plans to increase it and develop and implement its cloud strategy. The MTIT's current activities also include setting up a disaster recovery site outside the WB&G in Jordan. Several government sites do not implement basic security measures, such as the use of SSL, even if these sites include authentication (for example, see the open data portal).⁹⁹

Disaster recovery is the Government Computing Centre’s responsibility. However, there is currently no implementation for this. Disaster recovery is expected to be hosted outside of Palestine, in Jordan.

There is a requirement for SSL and penetration testing for all services developed since 2020, but older infrastructure has not been updated and not all services seem to follow the requirements. The open data portal is an example of a site with no SSL implementation.

There is a de facto “on-shoring/localization” policy to store government data within the Palestinian territories with the sole exception of e-School, the electronic education management system, the related data of which are stored on Azure cloud.¹⁰⁰

The information security policy places the responsibility for all backup requirements on the individual MDAs. Based on the interviews conducted during the field visit, this appears to be reasonable, with both on- and off-site backups.

**CONCLUSION**

Current information security policy defines a high-level framework to address data security, including backup procedures and data protection (physical protection). MDAs are responsible for adopting and adapting this policy to their needs.

MDAs appear to have good systems management practices; however, there is a continuing cost in duplicated systems engineering and management and a severe risk from a lack of disaster recovery planning. While these could be mitigated through migration to the MTIT cloud (or to other secure data centers that are available within some MDAs), the driver for migration will be more compelling once the shared cloud includes dedicated disaster recovery systems.

---

⁹⁸ World Bank Digital Economy Assessment and World Bank Cloud Readiness Assessment.
¹⁰⁰ This exception is due to the government data center being unable to meet e-School’s low latency and high concurrency requirements.
CONCLUSION

The assessment has examined different dimensions that may support or inhibit public sector data management, sharing, and reuse. Based on the core components required for data governance (see diagram below), the study has identified existing and missing elements.

The analysis of different dimensions of this study provides a mixed picture. The PA is interested in and has mobilized resources for the development of the digital economy. It has invested in important components, such as an e-government framework and an open data initiative. The NSO invests in the production of national statistics and SDG data. In all these areas, the PA—more specifically the MTIT and PCBS—consider and adopt international best practices and recommended tools and approaches. For example, open datasets and statistics are released with a CC-BY data reuse license, and open datasets are released in CSV format. They perform particularly well on some international indexes, such as ODIN and the WB SPI.

However, these activities do not always produce the expected outcomes. On the statistics side, the PCBS is a robust statistical office producing quality national statistics, and staff is appropriately skilled, with a clear set of policies defining a robust context for data sharing, publication and reuse. Progress on availability of timely quality statistics is recognized by non-government stakeholders. However, while production and dissemination of statistics is robust, the study could not capture evidence of the use of these statistics within MDAs for policy- or decision-making.

In e-government, a solid technical stack with Zinnar and UXP/X-Road and the one-stop-shop portal for e-services (Hukumati) provide a framework for all MDAs to access and share data for transactional operations. Hukumati has increased momentum within MDAs to invest in the development and release of e-services to citizens. This process is currently limited by a lack of e-signature implementation, which prevents the legal equivalence of electronic documents and requires people to visit an office to get a hand-signed document at the end of an e-service transaction. The lack of a unified business register prevents development of G2B e-services.

Despite the success of Hukumati, Zinnar, and UXP/X-Road and the development of e-services, these have not led to robust data management processes and data governance frameworks within MDAs. With the exception of specialized MDAs such as the MTIT and PCBS, most MDAs interviewed during the field visit do not consider data as a critical asset, but rather as a technical matter for their IT departments. This results in MDAs implementing limited data management practices. For example, no MDA maintains a data inventory, and most do not conduct routine data analysis. The limited capacity further risks the operational continuity of several data systems maintained by specific individuals on platforms where they are the only ones with knowledge to operate and maintain them without systemic processes for sustaining the technical skills and knowledge. Also, except for transactional data shared via X-Road/UXP, there is limited data sharing between MDAs.

The limited data use in the public sector is driven by the following two factors:
• **Lack of an enabling legal framework**: Sharing data requires a dedicated legal framework that supports classification of data assets and determines who has access and the method of treatment before sharing. The absence of legislation for data classification, personal data protection, and ATI precludes this classification process. In the absence of these components, each MDA defines its own internal procedures, which are not necessarily consistent with others.

• **Long, ad hoc data request procedure**: Owing to the lack of an enabling legal framework for data classification and of a data inventory that would identify available data and state the classification of each data asset, each data request procedure—whether from another MDA or from a non-governmental entity—is long and unpredictable. Each request usually requires ministerial approval, which then is translated into an MoU and transmitted to the IT department for data extraction and sharing. This process limits access to and reuse of public sector data.

Coupled with the limited institutional capacity, these bottlenecks also explain why there are only 39 datasets available despite heavy investment in the development of the Open Data Initiative, with an open data policy that implements international best practices, an open data portal, and data training. Published datasets usually contain historical data in an aggregated format, making them of limited reuse potential.

It is important to note that the interviews demonstrated that a local authority such as the RM has a vision for and is investing significantly in data management and reuse. However, it is currently limited by its inability to access government data, leading to duplication of efforts and duplication of e-services entry points for citizens. While the example of the RM does not represent the situation in other municipalities, it is worth noting its use of data and integration of data in decision-making, which significantly contributed to the development and delivery of e-services to Ramallah residents. The integration of local authorities into the government framework (X-Road/UXP, Hukumati, open data portal) is an opportunity for the central government to support municipalities and provide benefits to all stakeholders—from citizens to businesses, MDAs, and local authorities.

Finally, from an infrastructure perspective, the development of a government cloud is a positive step toward secure data hosting and easier data access and sharing. However, the lack of a disaster recovery site is a major point of failure, and a greater centralization of data in the government cloud and a greater use of data will increase the risks linked to the lack of such a recovery center. In the same way, the absence of a legal framework for data classification will slow and limit data migration to the government cloud.
STAKEHOLDER MAPPING

This section presents the stakeholders identified as part of this assessment and their role and responsibilities in implementation of the data governance framework. Some have a specific role (for example, coordination) and others are potential champions who could serve as agents of change and shining examples for others. For the latter, the list of identified champions within and outside government is unlikely exhaustive and only based on interviews conducted during the field visit.

KEY PUBLIC SECTOR PLAYERS

The core actors with regards to the data governance framework are:

• **MTIT:** The MTIT has a coordination and leadership role in most of the components of the data governance framework. It manages and drives the development of the following components:
  - E-government with a dedicated team for Hukumati, X-Road/UXP, and Zinnar. The MTIT chairs the corresponding steering committees (see the next section).
  - Open data with a dedicated team that supports MDAs. The MTIT national open data coordinator chairs the ODSC (see next section).
  - Artificial intelligence with the development of an AI strategy.

The MTIT is also driving work on the personal data protection bill and is liaising with the PMO for its adoption. It would also be a natural champion for a data classification bill, but work has not yet started.

• **PCBS:** The Palestinian General Statistics Law 4 of 2000 establishes regulatory frameworks for the PCBS as an NSO with independence and responsibility for providing statistical data to inform government and the public, including a data stewardship role across government. The PCBS set out its vision for data stewardship in the Palestine Data Strategy 2022–2026 with the goal of realizing more value in data within the national statistical system and increasing the use of statistical data in evidence-based decision-making. The PCBS is working closely with other MDAs through the established statistical units instituted by the statistics law. The PCBS Data Strategy 2022–2026 includes the development of a national business register.

• **MoI:** The MoI oversees the population register which is today the most used and largest data register shared on X-Road/UXP and is used by a large number of MDAs.

• **MoF:** The MoF is driving the Hukumati initiative and is one of the government's biggest data producers. Its political weight will be critical for implementation of the proposed action plan.

• **MoM:** The MoM has been involved in ATI activities and has been the contact point for CSOs to discuss the bill. However, the MoM is not currently actively championing the drafting and adoption of the ATI bill.

• **PMA:** The PMA is currently developing its own business register, and it will be a key role player in the design and development of a global business register that will support G2B services on Hukumati.

The table below summarizes the key actors in the PA, their role and responsibilities, and their area of interest and expertise.
<table>
<thead>
<tr>
<th>MINISTRY</th>
<th>ROLE AND RESPONSIBILITIES</th>
<th>AREAS OF INTEREST &amp; EXPERTISE / AREAS OF POSSIBLE CONTRIBUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTIT</td>
<td>Management of X-Road/UXP Management of Hukumati Management of the Open Data Initiative</td>
<td>Personal data protection Data classification ATI</td>
</tr>
<tr>
<td>PCBS</td>
<td>NSO Business registry</td>
<td>Personal data protection Standardization of metadata Geospatial data Business register</td>
</tr>
<tr>
<td>MoF</td>
<td>Hukumati lead Management of government revenue and expenditure systems</td>
<td>Implementation of the action plan</td>
</tr>
<tr>
<td>MoI</td>
<td>Management of the population register</td>
<td></td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td></td>
<td>Personal data protection ATI</td>
</tr>
<tr>
<td>MoM</td>
<td></td>
<td>Personal data protection ATI</td>
</tr>
<tr>
<td>MoLG</td>
<td>Management of the geospatial portal (GeoMOLG)</td>
<td>Geospatial data Involvement of local authorities in the national data governance framework</td>
</tr>
<tr>
<td>Palestinian Land Authority</td>
<td>Management of the geospatial portal</td>
<td>Geospatial data</td>
</tr>
<tr>
<td>PMA</td>
<td>Business registry</td>
<td></td>
</tr>
<tr>
<td>MoH, MoE, and MoHE</td>
<td></td>
<td>Potential champions and early movers at the national level to implement recommended approaches in the action plan.</td>
</tr>
<tr>
<td>RM</td>
<td></td>
<td>Potential champion and initial municipality to test integration of local authorities into the e-government framework (UXP/X-Road and Hukumati)</td>
</tr>
</tbody>
</table>

**COORDINATION STRUCTURES AND COMMITTEES**

There are multiple governance structures and steering committees to coordinate activities across MDA on different aspects of the data governance framework. Concerning e-government, the following coordination mechanisms are in place:

- Since 2010, the ECG has been put in place. It is chaired by MTIT and includes representatives from 15 ministries as well as representatives from academia and the private sector (since 2016). The ECG meets every month.

- In 2014, the Higher Ministerial Committee chaired by the Prime Minister was set up to oversee the overall e-government strategy, coordinate and manage e-government budgets, integrate and redefine government policies and processes, endorse standards, and integrate schedules and plans.

- The development of Zinnar is also driven by the National Interoperability Committee, which meets whenever there is new data to integrate in X-Road/UXP. The committee was set up again in February 2020 as a result of a Cabinet decision.101

---

101 [http://www.palestineCabinet.gov.ps/portal/Decree/DetailsEn/26110181-aa5a-4721-8c92-c7c55843d35f](http://www.palestineCabinet.gov.ps/portal/Decree/DetailsEn/26110181-aa5a-4721-8c92-c7c55843d35f)
Concerning open data, a national ODSC was formed in November 2018, established by a cabinet decision\(^{102}\) and chaired by the MTIT.\(^{103}\)

Concerning statistics, General Statistics Law (4) for Year 2000 requires all ministries to create a statistics unit.\(^{104}\) These statistics units coordinate their work with the PCBS, and the PCBS has the authority to request data from the various ministries to produce national statistics.

Finally, a “Technology and Public Administration” cluster was launched in March 2021 to drive the digital transformation of the Palestinian government together with the private IT sector.\(^{105}\) The cluster is led by a steering committee, chaired by the Secretary General of the CoM, and includes the MTIT, MoF, the Ministry of Entrepreneurship, MoE, MoHE, General Personnel Council, and the PMA. This committee is mandated to “discuss and construct strategies for building and directing a Palestinian ecosystem to assist in developing the sector in all its technical, legal, human and financial aspects.”

### NON-GOVERNMENTAL ROLE PLAYERS

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>TYPE</th>
<th>AREAS OF INTEREST / INTERVENTION</th>
<th>CURRENT OR POTENTIAL ROLE IN THE DATA GOVERNANCE FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palestinian Information Technology Association of Companies</td>
<td>Association/NGO</td>
<td>ICT sector</td>
<td>Part of the ECG</td>
</tr>
<tr>
<td>Leaders International</td>
<td>Association/NGO</td>
<td>Digital entrepreneurship</td>
<td>Part of the ODSC</td>
</tr>
<tr>
<td>Higher Council of Innovation and Excellence</td>
<td>Association/NGO</td>
<td>Innovation &amp; entrepreneurship</td>
<td></td>
</tr>
<tr>
<td>The Center for Continuing Education at Birzeit University</td>
<td>Academic</td>
<td>Open data</td>
<td>Support MTIT on open data</td>
</tr>
<tr>
<td>The Media Centre at Birzeit University</td>
<td>Academic</td>
<td>ATI Personal data protection</td>
<td></td>
</tr>
<tr>
<td>Good Shepherd Engineering</td>
<td>Private Sector</td>
<td>Geospatial</td>
<td>Support the Palestinian Land Authority in designing a new government geospatial portal</td>
</tr>
<tr>
<td>AMAN</td>
<td>Coalition of NGOs</td>
<td>ATI Personal data protection</td>
<td></td>
</tr>
<tr>
<td>MADA</td>
<td>Association/NGO</td>
<td>ATI Personal data protection</td>
<td></td>
</tr>
<tr>
<td>7amleh - The Arab Center for the Advancement of social media</td>
<td>Association/NGO</td>
<td>ATI Personal data protection</td>
<td></td>
</tr>
<tr>
<td>Momentum Labs</td>
<td>Private sector</td>
<td>Data analytics Entrepreneurship</td>
<td></td>
</tr>
<tr>
<td>Palestine Economic Policy Research Institute</td>
<td>Association/NGO</td>
<td>Research</td>
<td></td>
</tr>
</tbody>
</table>


\(^{103}\) Originally, the ODSC had 11 ministerial members. It now has 18 members, including non-governmental actors.


PROPOSED ACTION PLAN

GLOBAL OBJECTIVES OF THE PROPOSED ACTION PLAN

The following proposed action plan is structured based on the different themes of the assessment (ATI, data classification, data management, open data, e-government framework, e-transactions, personal data protection, and cybersecurity) and into short-, medium-, and long-term activities. These proposed activities seek to enable the establishment and implementation of a robust data governance framework to promote public sector data reuse within the government and by non-governmental actors.

PREREQUISITES

The core objective of a data governance framework is to promote public sector data use, reuse, and sharing by the Palestinian public administration and by non-governmental actors. It should also be guided by a once-only principle to reduce duplicated infrastructure and efforts by citizens and businesses.

However, greater use of centralized and single-source data will increase the importance of and load on the infrastructure hosting these data resources and platforms. It is critical that this infrastructure be redundant and secure to avoid creating a single point of failure that may endanger government services and the overall approach and initiative. As a significant part of the government data is planned to be hosted on the government data center, a disaster recovery center for this infrastructure is a prerequisite to all actions proposed in this action plan. In the same way, MDAs that have their own data infrastructure should ensure that they also have a disaster recovery site that could leverage the government data center.

ACTION PLAN STRUCTURE

The proposed action plan is divided into four areas to address the identified challenges and leverage strengths and opportunities. Each area is further divided into short-term (in the next 18 months), medium-term (to be launched in 18 to 36 months) and longer-term (action to be launched after 36 months) actions.

• Strengthening an enabling policy, legal, and regulatory environment: This area includes actions to strengthen the data governance policy, legal, and regulatory environment regarding three main topics: ATI and data request management, personal data protection, and data classification. In the short term, the objective is to provide a consistent framework for MDA compliance that will be adopted on a voluntary basis. In the medium/long term, the ultimate goal is to ensure that corresponding legislation is in place and enforced at each and every MDA. This component also includes recommendations on e-signature implementation to support the delivery of full online services through Hukumati.

• Building data management capacity: The second area of the proposed action plan aims to support MDAs in the implementation of robust data management processes. This includes building staff capacities in data management, use, sharing, and publication, increasing the availability of technical resources, and putting in place an M&E plan to track implementation.

• Implementing technical enablers: The third area of the proposed action plan identifies core technical enablers that will support MDAs in their data sharing and data publication endeavor. In the short term, this includes the setup of data inventories, the design and adoption of a data management technical framework and data standards, and the update of the open data portal. In the medium term, this includes the identification of data systems at risk and securing them.
**Strengthening collaboration and facilitating change management:** The last area of the proposed action plan includes recommendations that will help MDAs use more data in their activities and be more efficient and impactful in the way they engage with their data users. This includes a new internal organizational setup, the development of cooperation structures between MDAs and with non-governmental actors, and the development of use cases to demonstrate the power of data-driven decision-making processes. This component also includes recommendations to support greater use of data within society at large.

---

**SUBNATIONAL DATA GOVERNANCE FRAMEWORK**

The deployment of a national data governance framework at the subnational level is critical as local services and local data are the point where most citizens access e-government data and operational interactions take place.

Municipalities will store and use personal and commercial data as part of delivering their policy mandates. They are no less exposed to the risks and costs of data protection, infrastructure duplication, and resource constraints than their national government counterparts. They must provision these data resources in some form.

While the core focus of this assessment is on the national-level data governance framework, the field visit has demonstrated an opportunity to expand the data governance framework to municipalities, such the RM, which has already developed sophisticated data infrastructure and could interoperate with national government systems.

Not doing so already has a potential negative impact on financial and resource costs through the duplication of efforts, thus hurting state efficiency and significantly reducing accessibility and usability for citizens.

The RM is a significant outlier and not representative of Palestinian municipalities in terms of its human, financial, and technical resources. However, the RM has the technical and resource capacity to collaborate with the national government to investigate and develop standardized tools and processes to support overall municipal integration into the national data framework.

Lessons which emerge from such integration can then be extended to others that will likely need greater support (technical, infrastructure, and resources) to follow the same integration. In the future, the MTIT and PA may want to explore and resolve challenges with the RM, develop a standardized resource toolkit, and test and reproduce it in other municipalities. However, these recommendations fall outside the scope of this assessment and would require the amendment of local government laws that do not consider municipalities as government entities.

---

**DETAILED PROPOSED ACTION PLAN**

**STRENGTHENING ENABLING POLICY, LEGAL, AND REGULATORY ENVIRONMENT**

**SHORT-TERM ACTIONS**

- **Develop a limited data classification policy and guidance** focused on three levels (internal/shareable/publishable)\(^{106}\) based on international best practice.
  - **Rationale:** Data classification legislation is an important enabler to support data sharing between MDAs and data for public release. However, the drafting, adoption, and implementation of such legislation will take time. In the interim, given demand by MDAs for process guidance, it would be useful to define minimum data classification rules to support data sharing and then adopt them in a policy that could be applied on a voluntary basis by MDAs.
  - **Key role players:** MTIT, PCBS, MoM
  - **Time required:** 3–4 months to finalize guidance and building consensus.

---

\(^{106}\) The three recommended levels are the minimal number of levels required to support data sharing within the government and with non-governmental actors.
• **Indicative costs:** Around US$30,000 to US$40,000 for international expert support.

• **References:**
  - US\textsuperscript{107}
  - NATO\textsuperscript{108}
  - Saudi Arabia\textsuperscript{109}
  - Jordan\textsuperscript{110}

- **Develop a data request policy and guidance.** This policy should establish a formal process for responding to data requests based on the classification of data in the data inventory.

  • **Prerequisite:** Data classification and guidance are finalized. Data inventories are in place.

  • **Rationale:** The objective of this action is to ease and accelerate internal and external data request procedures at MDA level based on the classification of data assets in the inventory. This will provide a consistent policy across MDAs that will resolve the current administrative burden of securing management approval for each and every request and signing dedicated MoUs. This policy would be applied on a voluntary basis by MDAs and would provide for process similar to ATI legislation but dedicated to data and simplified through the use of a data inventory.

  • **Key role players:**\textsuperscript{111} MTIT, PCBS

  • **Time required:** 3–4 months to finalize guidance and building consensus.

  • **Indicative costs:**\textsuperscript{112} Around US$30,000 to US$40,000 for international expert support.

  • **References:**\textsuperscript{113}
    - Mexican General Act of Transparency and Access to Public Information\textsuperscript{114}
    - List of world ATI legislation and related evaluations\textsuperscript{115}

• **Develop personal data protection policy and guidance** that unify existing elements from other regulations and legislation, such as the PCBS privacy policy, the cybercrime law, and the Open Data Policy, and providing consistent guidance on how to manage personal data protection:

  • **Rationale:** A consistent process and robust legislation to manage and protect personal data is a key enabler for data sharing and a key element of trust for citizens. However, the adoption and implementation of such legislation will take time. In the interim, given demand by MDAs for process guidance, it would be useful to define data protection guidance and adopt it as a policy that could be applied on a voluntary basis by MDAs.

  • **Key role players:**\textsuperscript{116} MTIT, PCBS, MoM

  • **Time required:** 3–4 months to finalize guidance and building consensus.

\textsuperscript{107} https://www.archives.gov/ipsa/policy-documents/cnvi-eo.html.
\textsuperscript{109} https://sdaia.gov.sa/ndmo/Files/PoliciesEn005.pdf.
\textsuperscript{111} Stakeholders that should be involved in the activity because it is part of their mandate or because they have specific expertise required for the activity.
\textsuperscript{112} Indicative costs for the implementation of the activities. These do not include government staff time and only external costs such as the hiring of international experts, logistics, etc.
\textsuperscript{113} References of the implementation of similar activities in other countries.
\textsuperscript{115} https://www.rti-rating.org/.
\textsuperscript{116} Stakeholders which should be involved in the activity because it is part of their mandate; or because they have a specific expertise that is required for the activity.
Indicative costs:
Around US$30,000 to US$40,000 for international expert support.

References:
- EU General Data Protection Regulation
- OECD Privacy Principles
- Council of Europe Convention 108

**MEDIUM-TERM ACTIONS**

- **Finalize and effectively implement e-signatures** as part of the e-transaction legislation to increase the scale-up of Hukumati:
  - **Rationale:** Implementing and adopting e-signature will enable the delivery of public e-services online at their full potential, allowing citizens and businesses to fully conduct their requests online and get the documents they need without physically visiting a government office.
  - **Key role players:** MTIT
  - **Time required:** 9–12 months to finalize the revision of the e-transaction law and implementing e-signature.
  - **Indicative costs:** Costs of the implementation of e-signature infrastructure depending on the technical solution selected and adoption costs (awareness raising, training, etc.).

- **Develop, adopt, and implement personal data protection legislation:**
  - **Rationale:** The adoption of comprehensive personal data protection legislation is a critical element to provide a mandatory consistent framework in the way MDAs manage and protect personal data and its impact on data sharing.
  - **Key role players:** MTIT, PCBS, MoM, non-governmental stakeholders
  - **Time required:** 6–8 months to finalize the ongoing legislation process and launch implementation (setting up the DPA).
  - **Indicative Costs:** N/A, the drafting costs are currently covered by the MTIT in an ongoing process.
  - **References:**
    - EU General Data Protection Regulation
    - OECD Privacy Principles
    - Council of Europe Convention 108

- **Develop, adopt, and implement data classification legislation:**
○ **Rationale:** Adoption of comprehensive data classification legislation is essential to support the data governance framework and provide a consistent framework for MDA compliance. The data classification legislation should be developed as an enabler for the future ATI legislation and cover all the exceptions that impact the classification so that the process of designing the ATI legislation will be simplified and rely on this legislation.

○ **Prerequisite:** The current legislative process requires that the legislation has a clear champion to drive the drafting process and adoption through the PMO.

○ **Key role players:** MTIT, MoM, MoI, MoD

○ **Time required:** 4–6 months to draft the legislation

○ **Indicative costs:** Around US$40,000 to US$50,000 for international expert support to draft legislation based on international best practice.

○ **References:**
  - US legislation
  - NATO policy
  - Saudi Arabia legislation
  - Jordan legislation

**LONG-TERM ACTIONS**

- **Develop, adopt, and implement ATI legislation:**

  ○ **Rationale:** Adoption of comprehensive ATI legislation is essential to support the data governance framework, enable non-governmental stakeholders to request data, and provide a consistent framework for MDA compliance. The design of the ATI legislation should rely on the data classification legislation for coherency and to simplify the overall design process.

  ○ **Prerequisite:** The identification of a champion (likely between the MTIT and MoM) and its commitment is a prerequisite to this action. The adoption of the data classification legislation.

  ○ **Key role players:** MTIT, MoM, non-governmental stakeholders

  ○ **Time required:** 6–8 months to draft legislation and build consensus with non-governmental stakeholders.

  ○ **Indicative costs:** Around US$40,000 to US$50,000 for international expert support to draft legislation based on international best practice.

  ○ **References:**
    - Mexico General Act of Transparency and Access to Public Information
    - List of world ATI legislation and related evaluations

---

130 Inputs from and consensus with active non-governmental actors on the topic should be included in the process. See the stakeholder mapping section for relevant non-governmental actors.
BUILDING DATA MANAGEMENT CAPACITY

SHORT-TERM ACTIONS

• **Build a fellowship program:**
  - **Rationale:** One way to address the challenges of a limited number of staff, limited skills, and high staff turnover is to leverage external skills through a fellowship program to provide experience to young skilled professionals while helping MDAs access human resources at a lower cost.
  - **Key role players:** Birzeit University, MTIT, MDAs
  - **Time required:** 4–6 months to design the fellowship program and launch recruitment.
  - **Indicative costs:** Around US$100,000 to US$150,000 per year for a cohort of 40–50 fellows.
  - **References:**
    - US Presidential Innovation Fellows program
    - MCC Data fellowship program in Côte d'Ivoire

• **Develop a comprehensive training plan for government staff:**
  - **Rationale:** MDA staff need role-specific data management skills:
    - Managers and directors need to understand the value of data in analysis and decision support.
    - Data manager needs to know how to support data publication, analysis, use and reuse, etc.
    - Chief Data Officers (CDOs) need to know how to establish, develop, and maintain data inventories and to ensure documentation, process development, succession planning, etc.

  The aim of this action is to propose a comprehensive training plan which includes, but may not be limited to, the following topics:
  - Change management
  - Legal compliance
  - Data publication
  - Data analysis and visualization
  - Data inventory
  - **Prerequisite:** Data request, data classification, and personal data management guidance are adopted. Data inventory framework is finalized. Data management technical framework is adopted.
  - **Key role players:** MTIT, MDAs

---

133 [https://presidentialinnovationfellows.gov/](https://presidentialinnovationfellows.gov/)
Proposed Action Plan

- **Time required:** The program should be organized in short thematic sessions (two to five days) and run regularly (once or twice a year). Curriculum development will take around two to three months.

- **Indicative costs:** Development of the curriculum should cost around US$60,000 to US$70,000. Execution (logistics and trainers) should cost around US$10,000 to US$20,000 (international trainers for the higher bound) per session, that is, around US$50,000 to US$100,000 per cycle.

- **References:**
  - Open Data Dives in Tanzania

- **Develop an M&E plan for data management:** data inventory, data sharing, data publication/data reuse, e-services, and use cases:

  - **Rationale:** It is critical to establish an inclusive M&E plan to follow the progress of MDAs toward implementation of the data governance framework in all its dimensions.

  - **Key role players:** MTIT

  - **Time required:** 3–4 months to design the M&E plan.

  - **Indicative costs:** Around US$30,000 to US$40,000 for international expert support to design the plan, indicators, and measurement processes.

  - **References:**
    - Ireland Open Data Initiative M&E plan
    - Ethiopia Open Data Initiative M&E plan (section 7 of the draft Open Data Policy)

### IMPLEMENTING TECHNICAL ENABLERS

**SHORT-TERM ACTIONS**

- **Develop data inventories within MDAs.** Data inventories are the first and most important requirement for identifying data assets and supporting their reuse. Developing data inventories includes different activities:

  - **Define a data inventory framework and guide:**

    - **Rationale:** MDAs require clear and structured guidance for creating and maintaining their data inventory. As a first step, it is essential to define a data inventory framework (scope, metadata definitions, strategy, processes, management, resource requirements, data sharing platform) and produce an implementation guide for MDAs.

    - **Prerequisite:** A data inventory process includes classification of data assets. The completion of the framework and guide will require that guidance for personal data protection and data classification be available.

---


- Key role players: MTIT, PCBS
- Time required: 3–5 months to establish a dedicated working group, build consensus on the framework, and finalize the guide.
- Indicative costs: Around US$40,000 to US$50,000 for international expert support for the development of the framework and the guide.
- References:
  - USA Data Inventory Guide
  - Switzerland Data Inventory Guide
  - Canada Inventory
  - Example of a public data inventory: Washington, DC
  - Johns Hopkins University’s Center for Government Excellence (GovEx lab) Inventory Guide
  - San Francisco Inventory Guide

○ Train MDAs’ Chief Data Officers (CDOs):
  - **Rationale:** The data inventory guide will not be enough. It is essential to build momentum between MDAs by organizing training sessions on the use of the guide.
  - **Prerequisite:** The data inventory guide has been released and MDA CDOs have been nominated.
  - **Key role players:** MTIT, all MDAs
  - **Indicative costs:** Around US$50,000 to US$60,000 to organize a series of training sessions with international trainers and support CIOs in their data inventory journey.

- **Develop data management technical framework and data standards** (including metadata) for open data publication:
  - **Rationale:** The Open Data Policy provides high-level directives for data publication. However, these directives cannot be readily translated into practical publication guidance. To ease MDAs’ data publication, ensure consistency between publication, and facilitate the search, identification, and use of data, it is critical for MDAs to have clear instructions on, for example, minimum metadata requirements or data standards to follow. These standards should be aligned with and derived from Zinnar. In some cases, that may mean standardizing metadata and adding it to Zinnar as a resource.
  - **Key role players:** MTIT, PCBS
  - **Time required:** 3–5 months to develop guides and for ODSC to validate them.
  - **Indicative costs:** Around US$40,000 to US$50,000 for international expert support for development of the guides.
• Update the open data portal:
  ○ Rationale: The open data portal would benefit from features such as a dataset feedback module, a data request module (which could be designed to support the data request policy), or a more complete metadata schema. Other functionalities, such as a data validation module, could also provide useful tools for quick evaluation of data quality. Finally, the redesign of the home page would help promote new publications and the most popular datasets and could also promote data reuse. The update should also include the implementation of MTIT-required security measures such as the use of SSL.
  ○ Key role players: MTIT
  ○ Prerequisite: The portal should implement the metadata schema that will be adopted as part of the data management technical framework and should enforce the use of adopted data standards.
  ○ Time required: 1–3 months to update the portal.
  ○ Indicative costs: Around US$20,000 to US$25,000 for international CKAN expert support for implementation and redesign of the open data portal.
  ○ References:
    ▪ CKAN configuration guide
    ▪ CKAN security guide
    ▪ CKAN extensions

MEDIUM-TERM ACTIONS

• Identify data and data systems at risk and secure them:
  ○ Rationale: Multiple data systems performing important functions are potentially at risk from numerous factors, such as using undocumented proprietary or obsolete software, or because there is no continuity plan in place for staff retirement or reassignment. The objective of this activity is to identify data systems at risk, document them, and design and implement recovery or amelioration procedures. Implementing this recommendation should also be combined with carefully evaluating the data infrastructure currently hosting government data sources and information systems to ensure optimal security requirements, particularly the availability of disaster recovery sites. Eventually, the next step should be to transition key data sources/information systems to a robust data infrastructure, such as the existing government data center, with appropriate disaster recovery sites.
Prerequisite: Data inventories are the tools that will support identification of these data systems at risk within MDAs.

Key role players: MTIT, MDAs

Time required: 3–6 months to identify data systems at risk. Securing these systems will be highly dependent on the nature of the risk.

Indicative costs: Costs are mainly IT staff, and potentially investments in new software or equipment, but these costs cannot be evaluated before the data systems at risk are identified.

• Identify and develop key reference data registers, such as addresses or businesses:

  Rationale: Shared data registers are extremely valuable for MDAs, with the best example being the MoI-managed population register widely used by other MDAs. Other data registers have the potential to play a similar role. For instance, a shared unique comprehensive company register will support the development of e-services for businesses. A centralized address register will support the development of e-commerce, for example.

  Key role players: MTIT, MDAs (each register requires the involvement of a specific set of MDAs).

  Time required: 6–12 months per register.

  Indicative costs: Development of a data register mainly requires cooperation and collaboration between MDAs (staff time), although there may also be field infrastructure requirements (integrating parallel and competing business registers, ensuring buildings are allocated addresses).

STRENGTHENING COLLABORATION AND FACILITATING CHANGE MANAGEMENT

SHORT-TERM ACTIONS

• Redefine the mandate of the existing national open data coordinator at the MTIT and open data coordinators within MDAs to create a dedicated executive data manager position: a government CIO and CDO position at MDAs:

  Rationale: For data management efficiency and consistency purposes, it is critical to have a position dedicated to data management to maintain a data inventory, ensure appropriate proactive classification, and support consistent data processes within the MDAs. This position should be an executive position centralized at the top level of the organization.

  Key role players: MTIT, all MDAs

  Indicative costs: No external involvement. The MTIT should define two job descriptions for a national CIO and MDA CDO and promote the nomination of CDOs within MDAs.

  Time required: 1–2 months to finalize job descriptions and 2–4 months for nominations.

  References:

  • Federal Chief Information Officer of the United States

---

150 [https://en.wikipedia.org/wiki/Federal_Chief_Information_Officer_of_the_United_States#:~:text=The%20federal%20Chief%20Information%20Officer%20President%20appoints%20the%20Federal%20CIO](https://en.wikipedia.org/wiki/Federal_Chief_Information_Officer_of_the_United_States#:~:text=The%20federal%20Chief%20Information%20Officer%20President%20appoints%20the%20Federal%20CIO)
• **Leverage exchanges and collaboration between MDAs** by establishing a CDO working group:
  - **Rationale:** It is critical to support cross-MDA knowledge exchange and learning on data management and data reuse. A working group which meets regularly, whether physically or virtually, to exchange ideas, successes, and challenges will support development of a data culture within MDAs.
  - **Key role players:** MTIT, all MDAs
  - **Time required:** 1–3 months to establish the working group and define its charter.
  - **Indicative costs:** US$10,000 to US$20,000 per year for logistics costs for face-to-face meetings.
  - **References:**
    - USA CIO Council²⁵³

• **Leverage data use through the development of use cases**
  - **Rationale:** The objective of this recommendation is to support development of use cases within MDAs so that they realize the potential of data for problem resolution and decisions support and appreciate the importance of data inventory and data sharing. The development of use cases should also include the organization of innovation events such as hackathons to support implementation of use cases with the help of citizens.
  - **Prerequisite:** The data management technical framework has been adopted and the data inventory activity launched.
  - **Key role players:** MTIT, MDAs
  - **Time required:** 4–6 months to identify and frame use cases and organize a hackathon.
  - **Indicative costs:** Around US$20,000 to US$30,000 will be required for international expert support for the development of MDAs use cases. Around US$15,000 to US$20,000 will be required for hackathon logistics.
  - **References:**
    - Saudi Arabia DigitalGov Hack²⁵⁴
    - Jordan Hackathon for Government challenges²⁵⁵
    - Tanzania Data Tamasha²⁵⁶

• **Develop a communication plan and engage with non-governmental stakeholders** to support public sector data reuse and promote data requests:

---

²⁵² [https://www.civilservicejobs.service.gov.uk/cr/index.csp?ID=c2Vzc2VzXZJubm8wYWJsZWJlOTNjdGZvaWQvdXNlcnNlYXJjaHNvbnRhaW5lX3ZpbGlnb24/dHlwZT1jb250ZXh0fGlyeXNjaGV5b3V0fGlyeXNjaGV5b3V0aW5lX2hhc2UiOntzPSJ5c2NvcmRzIiwiaXNzIjoiY29tZGl0cyIsImRldiI6Ijg4MDI4IiwicmVxdWVzdG9yIjp7Xl93cGFja291dC1vZmZpbGUiOjE2MTEwMTI4MjMatrixN2UxN2E1MTZiOGRhNWRlZjg1ZjI2OWJkYjQyZjU3YjU2YzI0ZjQ3NTllZGE2MzY1YjUwZjI3ZDQyODc0ZjIyMDk1NzE0Nzc2NDkmcmVxdWVzdG9yX2FkbWluZ190cmFucy1jcmVxdWVzdG9yX2FkbWluZ19lbmNvZGluZ3MiXX0=](https://www.civilservicejobs.service.gov.uk/cr/index.csp?ID=c2Vzc2VzXZJubm8wYWJsZWJlOTNjdGZvaWQvdXNlcnNlYXJjaHNvbnRhaW5lX3ZpbGlnb24/dHlwZT1jb250ZXh0fGlyeXNjaGV5b3V0fGlyeXNjaGV5b3V0aW5lX2hhc2UiOntzPSJ5c2NvcmRzIiwiaXNzIjoiY29tZGl0cyIsImRldiI6Ijg4MDI4IiwicmVxdWVzdG9yIjp7Xl93cGFja291dC1vZmZpbGUiOjE2MTEwMTI4MjMatrixN2UxN2E1MTZiOGRhNWRlZjg1ZjI2OWJkYjQyZjU3YjU2YzI0ZjQ3NTllZGE2MzY1YjUwZjI3ZDQyODc0ZjIyMDk1NzE0Nzc2NDkmcmVxdWVzdG9yX2FkbWluZ190cmFucy1jcmVxdWVzdG9yX2FkbWluZ19lbmNvZGluZ3MiXX0=)
²⁵³ [https://www.cio.gov/](https://www.cio.gov/)
²⁵⁶ [http://dcli.co/use-stories/](http://dcli.co/use-stories/)
○ **Rationale:** Data reuse requires that non-governmental stakeholders be made aware of the open data portal and the various opportunities to request specific data. It is critical to promote these resources and data reuse. The plan should include an official highly visible (re)launch of the Open Data Initiative.

○ **Prerequisite:** The open data portal has been redesigned. A critical mass of MDAs has commenced their data inventory and published useful datasets on the open data portal. Geospatial data, including addresses and points of interest, are public.

○ **Key role players:** MTIT

○ **Time required:** 1–3 months.

○ **Indicative costs:** Around US$10,000 to US$15,000 for logistics and publication costs.

**MEDIUM-TERM ACTIONS**

- **Establish a government/non-governmental stakeholder committee** that includes representatives of different role players and that will meet regularly to identify challenges and advocate for and leverage data reuse:

  ○ **Rationale:** To leverage government data reuse by non-governmental stakeholders, it is essential to have a coordination mechanism between these different groups, to identify and resolve challenges, and to prioritize data release. An effective coordination mechanism is a committee with representatives from the government and from different categories of non-governmental role players.

  ○ **Key role players:** MTIT, non-governmental actors

  ○ **Time required:** 2–4 months to establish the committee.

  ○ **Indicative costs:** Around US$5,000 to US$10,000 for logistics for meetings.

  ○ **References:**
    - UK Public Sector Transparency Board[^157]

**LONG-TERM ACTIONS**

- **Develop and establish a data innovation center** to leverage public sector data reuse:

  ○ **Rationale:** As public sector data availability and reuse will grow over time, it is important to establish an entity that could operate a long-term fellowship program; maintain curricula and training sessions; support government MDAs, subnational authorities, and non-governmental stakeholders in data innovation; and support startups.

  ○ **Key role players:** MTIT, non-governmental stakeholders.

  ○ **Time required:** around 12 months to establish the entity, around 36 months for sustainability.

  ○ **Indicative costs:** Around US$400,000 to US$500,000 per year for three to four years until the entity is sustainable.

  ○ **References:**

- Mobile Web Ghana\textsuperscript{158} has supported Ghana’s government in implementation of the Ghana Open Data Initiative since 2010
- Jakarta Open Data Lab\textsuperscript{159}
- dLab Tanzania\textsuperscript{160}

\textsuperscript{158} http://www.mobilewebghana.org/  
\textsuperscript{159} http://labs.webfoundation.org/  
\textsuperscript{160} http://www.dlab.or.tz/
## ANNEX I: SUMMARY OF PROPOSED ACTION PLAN

<table>
<thead>
<tr>
<th>Objective 1: Strengthening Enabling Policy, Legal, and Regulatory Environment</th>
<th>SHORT-TERM</th>
<th>MEDIUM-TERM</th>
<th>LONG-TERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1.1. Develop data classification policy and guidance</td>
<td>M1.1. Develop, adopt and implement data classification legislation (prerequisite: identification of a champion Ministry to drive the process)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S1.2. Develop personal data protection policy and guidance</td>
<td>M1.2. Develop, adopt, and implement personal data protection legislation M1.3 Finalize and effectively implement e-signatures</td>
<td>L1.1. Develop, adopt, and implement ATI legislation (prerequisite: M1.1, identification of a champion Ministry to drive the process)</td>
<td></td>
</tr>
<tr>
<td>S1.3. Develop data request policy and guidance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective 2: Building Data Management Capacity</th>
<th>SHORT-TERM</th>
<th>MEDIUM-TERM</th>
<th>LONG-TERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2.1. Build a fellowship program to address the challenges of capacity constraints</td>
<td>M3.1. Identify data and data systems at risk and secure them (prerequisites: S3.1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2.2 Develop a monitoring and evaluation plan for data management</td>
<td>M3.2. Identify and develop key reference data registers such as address and business registers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2.3. Build a fellowship program to address the challenges of capacity constraints (prerequisites: S1.1, S1.2., S1.3.)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective 3: Implementing Technical Enablers</th>
<th>SHORT-TERM</th>
<th>MEDIUM-TERM</th>
<th>LONG-TERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3.1. Develop data inventories within MDAs (prerequisites: S1.1, S1.3.)</td>
<td>M3.1. Identify data and data systems at risk and secure them (prerequisites: S3.1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3.2. Develop data management technical frameworks and data standards (including metadata) for open data publication</td>
<td>M3.2. Identify and develop key reference data registers such as address and business registers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3.3 Update the open data portal and expand its functionalities (prerequisites: S3.2)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective 4: Strengthening Collaboration and Facilitating Change Management</th>
<th>SHORT-TERM</th>
<th>MEDIUM-TERM</th>
<th>LONG-TERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S4.1. Redefine the mandate of existing national open data coordinator at MTIT and open data coordinators within MDAs to create dedicated executive data manager positions (e.g., Chief Data Officers)</td>
<td>M4.1. Establish a government/non-governmental stakeholder committee that meets regularly to identify challenges and facilitate data use</td>
<td>L4.1. Develop and establish a data innovation center</td>
<td></td>
</tr>
<tr>
<td>S4.2. Development of data use cases within MDAs (prerequisites: S3.1., S3.2.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4.3. Leverage exchanges and collaboration between MDAs through establishing Chief Data Officers (e.g., CDO) working group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4.4. Develop a communication plan and engage with non-governmental stakeholders</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ANNEX II: METHODOLOGY

The main objective of this study is to provide a qualitative assessment to support the Palestinian Authority (PA) in identifying key opportunities and challenges related to strengthening data regulatory frameworks and data practices in the public sector.

This study pilots the World Bank Global Data Regulation Toolkit, an integrated qualitative diagnostic tool that is designed to support a landscape analysis of a given country’s existing data regulation framework and practices that enable the effective and trustworthy usage of data for economic development purposes. The toolkit is structured around key “enablers” and “safeguards” needed to support countries’ transition to a data-driven and digital economy, and government and society that is based on trust, equity, and value. The methodology of the toolkit is intended to assess both “de jure” frameworks and “de facto” practices. The “de jure” information refers to data governance regulatory environments and the “de facto” information looks to measure the implementation effectiveness of data governance frameworks in use. Therefore, the survey covers not only laws and regulations on paper, but also information related to the implementation of legal and regulatory frameworks, such as the existence of relevant institutions to oversee or enforce legal rights and obligations.

To measure the effectiveness of these institutions and entities, the toolkit also includes diagnostic questions on characteristics of well-functioning institutions, including questions related to independence (where it is a criterion for functional effectiveness), budgetary and human resources, the existence of robust monitoring and evaluation plans, and criteria around the transparency and accountability of information shared.

The structure of the toolkit is composed of pillars, dimensions, sub-dimensions, and assessment questions. The pillars are indicators that provide quantitative measurements of the laws and regulations and/or information related to their implementation. Pillars are categorized as enablers, safeguards, and technology-specific questions, and are integrated by different dimensions, which in turn comprise a variety of sub-dimensions. The toolkit is modular where pillars and dimensions can be selected for a specific study based on the objectives of the assessment. In the case of the assessment for the Palestinian Authority presented in this report, the focus is on public sector data use, reuse, and sharing.

The following pillars and dimensions have been selected:

- Enablers
  - E-transactions
    - Legal equivalence
    - E-signature
    - Digital ID
  - Public sector data enablers
    - Data production, management & sharing
    - ATI
    - Data Classification

Based on the definition in the World Development Report 2021: Data for Better Lives
• Open Data

• E-Government framework
  • Interoperability of data and systems

• Safeguards
  ○ Personal data protection
    • Legal framework
    • Technical and organizational standards
    • Coordination with other legal regimes (e.g., national statistics, open data, ATI)
    • Institutional effectiveness
  ○ Data security:
    • Adoption of legal framework and technical standards
    • Institutional arrangements and technical capacity

Annex III lists the questions the assessment covered that were adopted from the Global Data Regulation Toolkit.
ANNEX III: GLOBAL REGULATION TOOLKIT
QUESTIONNAIRE USED IN THIS ASSESSMENT

LEADERSHIP

DIGITAL TRANSFORMATION, DIGITAL ECONOMY, DIGITAL GOVERNMENT
• What is the importance of digital transformation/digital economy at the government level? What is the vision? What are the objectives?
  ○ What is the vision at the Government level on the role of data in the digital transformation/digital economy?
  ○ What is the vision on public e-services?
  ○ What is the vision on the role of digital in government (G2G, G2B, G2C)?

DATA FOR DECISION-MAKING, OPEN DATA
• What is the vision at the government level and at MDA top management on the role of data in governance, decision-making, policy making and policy evaluation? Is their awareness and interest in Open Data?
  ○ Is there a strong demand from management for statistics, data analysis, and quantitative dashboards? AI?
  ○ What is the importance of Monitoring and Evaluation? Importance of SDGs?

INNOVATION & ENTREPRENEURSHIP
• What is the importance of ICT Innovation/Startup at Government?
  ○ What is the importance of the development of online services and e-commerce?

OPEN GOVERNMENT, TRANSPARENCY, ACCOUNTABILITY
• What is the importance of transparency/accountability/Open Government?
  ○ Is there any plan to join the Open Government Partnership?

CYBERSECURITY & DATA PROTECTION
• What is the vision on cybersecurity and protecting/safeguarding government information systems and government data?

PERSONAL DATA PROTECTION
• What is the vision on personal data protection and its importance in digital/online services?

COORDINATION MECHANISMS
• What are coordination mechanisms and governance structure in place related to data governance?
ACCESS TO INFORMATION

LEGAL & POLICY FRAMEWORK

• Has ATI legislation been passed that grants individuals the right to request government records or data? If not, what are relevant past and ongoing activities?
  ○ Does the law implement the open by default principles? Does the law provide for limitations or exceptions to this right of requesting access to government records or data?
  ○ Does the law include a provision for proactive disclosure of government information? Does it criminalize the use or reuse of government information received? If so, under what conditions?
    ▪ Does it provide reuse rights?
    ▪ Does the law include a provision requiring the collection of data on ATI requests?
    ▪ Number of requests submitted?
    ▪ Number of requests accepted/rejected?
    ▪ Reasons for successful/unsuccessful request?
    ▪ Is this information published and publicly available on a citizen-facing government website?

INSTITUTIONAL SETUP

• Is there a centralized independent body to process ATI requests?
• Does each Ministry, Department and Agency include a focal point to process ATI requests?
  ○ Is the contact information for these focal points publicly available?

IMPLEMENTATION PRACTICES

• How is the ATI law evaluated on international indexes?
  ○ Global Right to Information Rating
  ○ Other evaluations (Article 19, NGOs, international actors...)
• How do MDAs manage information request?
  ○ From the perspective of the MDA
  ○ From the perspective of requesters (non-governmental actors)
• Is there any CSO coalition to promote ATI?
• What is their evaluation of the effectiveness of the legislation?
DATA CLASSIFICATION

LEGAL & POLICY FRAMEWORK

• Is there a government data classification policy/directive?
  ○ Does the policy or directive prescribe the categories of common data classification? How many levels of classification exist, and what are they?
  ○ Is it mandatory to use the common data classification categories across government database applications or document management systems?

• Is there any ongoing work related to data classification for the ongoing cloud migration?

CAPACITIES

• Is there a government-wide training program to train civil servants to apply the data classification policy to datasets within their remit?
  ○ How wide is the program?

IMPLEMENTATION PRACTICES

• How and when is managed data classification?
  ○ Who decides if and how data can be shared? Published?

• Are there global guidelines for data classification?

• How accurately are data classified from the perspective of non-governmental actors?

OPEN DATA

LEGAL & POLICY FRAMEWORK

• Is there an Open Data Act or open data policy applicable across the entire public sector? Or an open data section in the Access to information act?
  ○ At what level of government is this policy applicable (the entire public sector; central government; local government, ...)
  ○ Does the policy/law provide for the proactive disclosure of data? Does it permit the use and reuse of data for commercial purposes? Does it criminalize or otherwise limit the “misuse” of data? Or are there any other policies that prevent disclosure or reuse?
  ○ Does the policy include the setup and management of a data inventory?
    ▪ What is the scope of the inventory?
  ○ Does the policy include data update requirements?

• Is there a policy or regulation that defines the open data technical framework? Organizational framework? Legal framework (licenses, fees...)?
  ○ Has the government adopted an open licensing regime (such as a Creative Common License by Attribution or ODbL) to enable the reuse of public sector data?
- Does the Open License apply to all government data?
- Does the open license include a non-revocability clause? Does it permit reuse for commercial purposes?
  - Is there a law or regulation regulating the commercial use of public sector data?

INSTITUTIONAL SETUP

• Who are the agencies that drive the country’s OPEN DATA INITIATIVE?
  - What is the political weight of these agencies?

• Who is in charge of the portal?
  - Is there an “open data officer” or “open data custodian” (or similar role and structure) responsible for the curation, processing, quality assurance and maintenance of the open data portal?

• What is the organizational setup for the development of the Open Data Initiative
  - Are there data positions within MDA (e.g., CDO)?

• Is there an open data committee with different MDAs?

• Is there a formal coordination mechanism with non-governmental actors (OGP committed, open data committee...)?
  - If not, is there an informal mechanism for cooperation?

CAPACITIES

• What are portal management capacities of the agency in charge?

• What are data management capacities within MDAs?

• What are data publication capacities within MDAs?
  - What are anonymization capacities?

• What are data capacities and open data awareness within
  - CSO & Media
  - Innovation actors
  - Private sector
  - Research

• Is there ongoing government-wide awareness raising or training activities on data management/data publication/data use?

• Is there any awareness raising or training activities for non-governmental actors on public government data reuse?
IMPLEMENTATION PRACTICES

- Is the government proactively releasing open datasets and encouraging their reuse on an open data portal/platform (unique national portal/platform or national portal/platform linking to ministry or sector-specific portals)?
  - What are datasets available?
  - are the data published
    - Regularly maintained and updated? How frequently?
    - In a disaggregated format?
    - With accompanying metadata
    - In multiple and exploitable formats (e.g., .csv)? If not, in what formats are data published (word, pdf)
    - Available for bulk download?
    - Available for download via APIs?
  - How many published datasets are published under the terms of the open data license (or equivalent)?
  - Who are using the published datasets?
    - Are there MDA-generated use cases? Non-gov use cases?
  - Does the portal offer interaction mechanisms for users (and what is the effectiveness of these services)
    - Data requests
    - Comments on published datasets
  - Does the portal promote reuse/use cases?

- To what extent do MDAs have a coherent view of its data holdings? Did they put in place, and do they maintain an organization-wide data inventory?
  - What is the information collected as part of the inventory?
    - Descriptive metadata
    - Structural metadata
    - Administrative metadata
    - Classification information
  - What inventory criteria is used to prioritize for publication (e.g., “high value” datasets?)
  - Is the inventory public? Does it contain only public resources or all resources?

- How are structured/organized data assets within MDAs?
- How are prioritized datasets for publication? Are there specific types that are prioritized?
• How do MDAs manage data request?
  ○ From the perspective of the MDA
    • To what extent is government data sold by agencies
  ○ From the perspective of requesters (non-governmental actors)

• Do MDAs have communication channels and discussion with non-governmental actors?
  ○ What activities has the government engaged in to promote reuse of government-held data (e.g., in developing apps or organizing co-creation events)? How could such promotion be developed or enhanced?

• What is the state of the demand for data from non-governmental actors
  ○ CSO & Media
  ○ Innovation actors
  ○ Research
  ○ Private sector

NATIONAL STATISTICAL SYSTEM

LEGAL & POLICY FRAMEWORK

• Is there a National Statistics law or act of general application that governs the collection, processing, and use of statistical data?
  ○ In what year was the law last updated?
  ○ Does the law provide for the creation of a National Statistics Office (NSO)?
  ○ Do the National Statistics Office (NSO) and other institutions in the NSS have a clear mandate to collect personal and non-personal data from natural (individuals or households) and legal (e.g., firms) persons?
  ○ Does the law impose on the NSO a formal “data stewardship” or “data custodian” role for all public sector data?
  ○ Does the National Statistics law grant the NSO different powers over the collection, use and storage of personal data/personally identifiable information than the data protection law?
    • Does not allow for any other use other than for statistical purposes
    • Has Statistical disclosure controls in place for disseminating deidentified data
    • Disclose personal data when the individual has provided the data for statistical purposes consents for it to be used for other purposes (e.g., establishing a voters’ register).
    • Disclose data if it is to be used as evidence in a court of law
    • Disclose data when government entities have the right to access personally identifiable information (e.g., tax authority)
- Release data for the purpose of scientific research
- Release data in an emergency situation (e.g., public health crisis)
- Other
  - Does the National Statistics law (or other legal framework – please specify) guarantee the “professional independence” of the NSO?

**INSTITUTIONAL SETUP**

- Who is in charge of producing national statistics?
- Where is place the NSO in Government organogram?
- What is the organizational setup for production and dissemination of statistics?

**CAPACITIES**

- What are the capacities of the NSO (and staff profile)
  - Survey
  - Data management
  - Production of statistics
  - Anonymization
  - Big data
- What are capacities at MDAs to collect and manage data, and to produce statistics?
- Is there any awareness raising or training activities aiming at promoting the use of statistics by non-governmental actors?

**IMPLEMENTATION PRACTICES**

- How is evaluated the NSS in international index
  - World Bank Statistical Performance Indicators (SPI)
  - Open Data Watch Open Data Inventory index (ODIN)
- Are there specified arrangements (statistics law, technical committees, data sharing agreements) for administrative data sharing within the public sector (between NSO/institutions in NSS and other ministries)?
- In which format are national statistics provided?
  - In terms of disaggregation?
    - Geography
    - Gender
  - In terms of dissemination support (report, pdf, machine readable data)
  - In terms of reuse licenses
- Is there an internal or public inventory of all available national statistics?
• How does NSO manage data request?
  ○ From the perspective of the NSO
    ▪ For statistics
    ▪ For survey microdata
  ○ From the perspective of requesters (non-governmental actors)
  ○ Are there mechanisms in place to allow researchers access to restricted-use data?

E- GOVERNMENT FRAMEWORK

LEGAL & POLICY FRAMEWORK
• Is there a National Interoperability Framework?
  ○ Does the Interoperability Framework include mandatory provisions for:
    ▪ Legal interoperability
    ▪ Semantic interoperability (semantic vocabularies and syntactic formats)
    ▪ Technical interoperability (systems and protocols)
    ▪ Organizational interoperability
• What is legislation, policies and regulations concerning the interoperability platform?
  ○ Are all government agencies legally required to query data from basic registries/repositories rather than collect and hold their own data?
• Is a digital transformation? A digital government strategy?

INSTITUTIONAL SETUP
• Who is in the charge of the interoperability platform?
• Is there a specific organizational setup for the development and maintenance of e-services? For ICT matters in general?
• Who is charge of the key registries?
• Is there a central entity in charge of an e-services portal?
• Is there an entity in charge of supporting MDAs in the implementation of the interoperability platform and e-services?
• Who is in charge of the designing and maintaining the technical framework (e.g., metadata standards etc.)?

CAPACITIES
• What are the capacities of the entity in charge of
  ○ The interoperability framework?
• The interoperability platform?

• What are MDAs capacities related to implementing
  • The interoperability framework?
  • The interoperability platform?
  • E-government services

• Is there an entity in charge of building technical capacities of MDAs?

IMPLEMENTATION PRACTICES

• How is evaluated the development of E-government on international indexes
  • UN E-Government Development Index (EGDI)
  • OECD Digital Government Index

• Has the government adopted unified data standards (including reference data standards such as taxonomies, vocabularies, code lists and data structures, as well as metadata standards) that enable the interoperability of systems, databases, and data registries?
  • do these standards follow:

  • International conventions, such as W3C Dublin Core for georeferencing data, HL7’s FHIR for health data, SDMX for statistical data, DCAT vocabulary, etc.
  • Industry standards (ISO, IEEE, etc.)
  • Open specifications

• Does the government have established standards for Application Programming Interfaces (APIs) to develop applications or online services? Or more generally have adopted an interoperability platform?

• Has the Government defined, digitized, and shared a set of basic (reference) data registries/repositories? (List them and evaluate their completeness)
  • For each basic register, has the government defined institutional responsibilities for the operation, update, and sharing of the register's data?

• To which extend MDAs implements the interoperability framework, and successfully deploy the interoperability platform?

• To which extend are e-services end-to-end digital including payment and provision of e-document?

E-TRANSACTIONS

LEGAL & POLICY FRAMEWORK

• Is there a national e-commerce/e-transactions law or regulation?
  • Does the e-commerce/e-transactions law include provisions that grant legal equivalence between paper-based and electronic communications, contracts, signatures, and records?
  • Are there any documents that cannot be legally accepted in electronic format?
Does the law or regulation prescribe a specific form or condition for any of the following?

- **Is there an E-signature law or regulation?**
  
  - Are there any documents that cannot signed electronically?
  
  - Have relevant implementing regulations been adopted?
  
  - Which entities are authorized to issue digital certificates?
  
  - Do the law/implementing regulations provide for the creation of a Certification Authority (CA)?
    
    - Does the Certification Authority’s mandate include the following roles and responsibilities?
      
      - Issuing digital certificates
      
      - Authenticating and validating e-transactions
      
      - Managing or regulating PKI infrastructure
      
      - Is there a law or regulation that governs the creation and management of a government-recognized digital ID system?

- **Does this ID system provide a foundational credential to access government services?** (E.g., e-tax filing, online benefits application?)
  
  - If yes, is this credential:
    
    - Issued as a permanent identity number (unique identifier)
    
    - Randomly structured (or are there numbers or letters that could identify the individual’s legal status)

- **Does the ID law/regulation limit the number of data fields that can be collected or are these data fields specified in implementing regulations?**

- **Are there regulations that force all MDAs to use the E-id systems for identification and authentication in e-services?**

### INSTITUTIONAL SETUP

- **Who is in charge of digital signature infrastructure and oversight?**

- **Who is in charge of digital id infrastructure and oversight?**

### CAPACITIES

- **Is there any entity in charge of supporting the integration of Digital id within different MDAs?**

- **What are capacities of entities in charge of**
  
  - E-id platform
  
  - E-id management (enrollment etc.)
  
  - Digital Signature
IMPLEMENTATION PRACTICES

- **E-signature**
  - Have any certificates been issued for digital signatures (e.g., PKI)?
  - Have any licenses been issued for private CAs?
    - If yes, how many?

- **Legal equivalence**
  - How widely is used electronic format for official record (e.g., birth certificates, criminal records...)?

- **Digital ID**
  - How is Digital id used across multiple government database to link records to an individual?
  - Is the government-issued ID also used by the private sector?
    - Is there a cost associated?
  - To which extend e-id is deployed in all civil registry event (death, birth...)
  - What is the % of population enrolled on the e-id database?
  - How many services use digital id?
  - What there any awareness raising/ national campaign to promote Digital id?

PERSONAL DATA PROTECTION

LEGAL & POLICY FRAMEWORK

- Is there a data protection/privacy law of general application explicitly governing the use, collection, and processing of governing personal data (including sensitive data) and PII (“personal data”)?
  - If not, are there sector-specific personal data protection and/or privacy laws?
  - If no laws exist, have there been any significant court or administrative decisions that form the basis of or clarify privacy or data protection rights?
  - Were any of the below international/regional models or guidelines used as the basis for developing the data protection legislation or did the country signed any international treaty on personal data protection?
    - UN Personal Data Protection and Privacy Principles (2018)
    - EU General Data Protection Regulation (EU GDPR)
    - Commonwealth model law on privacy
• Does the scope of application of the law extend to:
  ○ Natural persons
  ○ Legal persons
  ○ Groups/collective entities

• Does the law or regulation apply to data processing taking place outside the country’s borders (extraterritoriality provision)?

• Does the law specify any exceptions to provisions regulating the collection, use or sharing of personal data? If yes, on which grounds?
  ○ National security
  ○ Law enforcement
  ○ Service delivery
  ○ Public interest (including public health)
  ○ Other

• To which parties do these exceptions to obligations apply?
  ○ Public sector entities/government
  ○ SMEs
  ○ Other categories of natural or legal persons

• Have relevant implementing regulations been adopted?

• Do the law or implementing regulations provide for the creation of a data protection authority (DPA) or equivalent?
  ○ does the DPA’s mandate include the following roles and responsibilities?
    ▪ Enforce rights and obligations enshrined under the data protection law or regulation
    ▪ Provide guidance on the interpretation of the data protection law or regulation
    ▪ Communicate and promote awareness of the risks, rules and safeguards of rights pertaining to personal data
    ▪ Encourage the creation of codes of conduct and review certifications
    ▪ Regularly publish activity reports
    ▪ Provide redress mechanism

• Does the law or regulation require the DPA to review and approve of data processing on an ex ante basis (before the processing can take place)?
  ○ Does this requirement apply to:
- Processing of “sensitive” personal data
- Automated processing of personal data
- All data processing
- Other

INSTITUTIONAL SETUP

- Has the DPA or equivalent institution been created within a year of the law or regulation being adopted?
  - In the absence of a DPA, is there another entity responsible for receiving complaints, conducting investigations, and applying remedies (including issuing fines)?
- Is the DPA involved in various projects technical committee to provide inputs on personal data protection?
- To support accountability at the organizational level, are public sector entities and firms responsible for appointing a data protection officer (DPO) responsible for undertaking risk assessments (e.g., DPIAs), monitoring and reporting data breaches to the entity leadership (e.g., CEO or board within private sector or ministry, head of agency or equivalent for public sector entities)?

CAPACITIES

- What are the capacities of the DPA?
  - Data Anonymization
- What are capacities and awareness within MDAs
  - On what is exactly personal data and how it has to be protected?
  - On obligations in terms of protection and appropriate transformation (anonymization) before publication?
  - On data anonymization techniques
- What are capacities and awareness within non-governmental actors
  - On what is exactly personal data and how it has to be protected?
  - On obligations in terms of protection and appropriate transformation (anonymization) before publication?
  - On data anonymization techniques

IMPLEMENTATION PRACTICES

- How do MDAs evaluate and manage personal data in datasets?
- What is the level of understanding of personal data protection within MDAs?
- How important and sensitive is the topic for MDAs?
CYBERSECURITY

LEGAL & POLICY FRAMEWORK

• Is there a national cybercrime & cybersecurity law and what is the status?
  ○ Is there a national cybersecurity policy?
  ○ Is there any specific regulation for public information systems that provide clear guidelines to MDAs on measure to undertake to preserve data integrity and security?

• Does the cybercrime law or other laws and regulations criminalize the following activities?
  ○ Criminalize unauthorized access to systems or other databases holding personal data?
  ○ Criminalize unauthorized interception of data from systems or other databases holding personal data?
  ○ Criminalize unauthorized damaging deletion, deterioration, alteration, or suppression of data collected or stored as part of databases holding personal data?
  ○ Criminalize unauthorized interference with databases holding personal data?
  ○ Criminalize the misuse of devices or data for the purpose of committing any of the above criminal behavior?
  ○ Criminalize unauthorized input, alteration, deletion or interference with a computer system or platform to procure an economic benefit which would apply to databases holding personal data?
  ○ Criminalize fraudulent use or alteration of data or interference with a computer system to procure an economic benefit which would apply to databases holding personal data?

• Do data processors/controllers have to comply with the following security requirements for the automated processing of personal data?
  ○ Encryption of personal data
  ○ Anonymization/pseudonymization of personal data
  ○ Confidentiality of data and systems that use or generate personal data
  ○ Integrity of data and systems that use or generate personal data
  ○ Availability of data and systems that use or generate personal data
  ○ Ability to restore data and systems that use or generate personal data after a physical or technical incident
  ○ Ongoing tests, assessments, and evaluation of security of systems that use or generate personal data
  ○ Other

• Do data processors/controllers have to comply with the following cybersecurity requirements?
  ○ Adoption of an internal policy establishing procedures for preventing and detecting violations
  ○ Confidentiality of data and systems that use or generate personal data
- Appointment of a personal data processing office/manager
- Performance of internal controls
- Assessment of the harm that might be caused by a data breach
- Awareness program among employees

Do the laws, implementing regulations or policy provide for the creation of a cybersecurity strategy, infrastructure, and institutions to identify, investigate, and address cyber-security threats?

Do(es) the law(s) provide for the creation of:
- A cyber-security plan to protect key national infrastructure
- A CERT/CSIRT that is capable and ready to prevent, respond and recover from cyber incidents

INSTITUTIONAL SETUP

What is the institutional organization to manage information protection, cybersecurity, and backup?
- Is there a network of local CERTs / cybersecurity focal points across public sector entities that monitor and report threats to the national CERT/CSIRT?

CAPACITIES

What are capacities of the agency in charge?

Is there awareness raising sessions for MDA staff?

What are MDA capacities to manage cybersecurity, define and implement procedure?

Are there any capacity building initiatives on cybersecurity?

IMPLEMENTATION PRACTICES

Is there a government data center?
- How widely is it used?
- Is there a disaster recovery center?

To which extend MDAs have cybersecurity procedures in place?
- Which systems are covered by those procedures?